APPROPRIATE USE POLICY
INFORMATION TECHNOLOGY

SCOPE

This Policy applies to all Users of Berean Christian High School Information Technology Systems, including but not limited to Berean students, faculty, and staff. It applies to the use of all IT Systems. These include systems, devices, networks, and facilities administered by BCHS. Use of IT Systems, even when carried out on a privately-owned computer that is not managed or maintained by Berean Christian High School, is governed by this Policy if it in any way makes use of the BCHS IT Systems.

POLICY STATEMENT

The purpose of this Policy is to ensure an information technology infrastructure that promotes the basic missions of BCHS in teaching, learning, and administration. In particular, this Policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and superior performance of IT Systems
- To ensure that use of IT Systems is consistent with the principles and values that govern use of school facilities and services
- To ensure that IT Systems are used for their intended purposes
- To establish processes for addressing policy violations and sanctions for violators

REASON FOR THE POLICY

Information technology (IT), the vast and growing array of computing and electronic data communications facilities and services, is used daily to create, access, examine, store, and distribute material in multiple media and formats. Information technology plays an integral part in the fulfillment of Berean Christian High School's overall educational goals. Users of Berean's IT resources have a responsibility not to abuse those resources and to respect the rights of the members of the community as well as the school itself. This Berean Christian High School IT Appropriate Use Policy (the "Policy" or "AUP") provides guidelines for the appropriate use of Berean's IT resources as well as for the school's access to information about and oversight of these resources. Most IT use parallels familiar activity in other media and formats, making existing school policies important in determining what use is appropriate. Using electronic mail ("e-mail") instead of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor does it alter the guiding policies. School policies that already govern freedom of expression and related matters in the context of standard written expression govern electronic expression as well. This Policy addresses circumstances that are particular to the IT arena and is intended to augment but not to supersede other relevant school policies.

For statements of other applicable BCHS policies, consult the Student and Faculty Handbooks as appropriate. Berean's Department of Information Technology Services has promulgated policies that govern the use of various IT Systems, such as Berean's World Wide Web site and IT Systems email services. Other IT service providers at Berean have also adopted policies governing use of systems they manage.

DEFINITIONS

- **IT Systems**: These are the computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by Berean Christian High School. For example, IT Systems include iPads, computers and the school's campus network.
- **User**: A "User" is any person, whether authorized or not, who makes any use of any IT System from any location. For example, "Users" include persons who access IT Systems in the school's computer cluster or via an electronic network.
- **Systems Authority**: While Berean Christian High School is the legal owner or operator of all IT Systems, it may delegate oversight of particular systems to the head of a specific department (Systems Authority), or to an individual faculty member in the case of IT Systems purchased with funds for which he or she is personally responsible.
- **Systems Administrator**: Systems Authorities may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular IT resources.
- **Certifying Authority**: This is the Systems Administrator or other school authority who certifies the appropriateness of an official school document for electronic publication in the course of school business.
- **Specific authorization**: This means documented permission provided by the applicable Systems Administrator.

POLICY SECTIONS

I. Appropriate Use of IT Systems

Although this policy sets forth the general parameters of appropriate use of IT Systems, students, faculty, and staff should consult their respective governing policy manuals for more detailed statements on permitted use and the extent of use that the school considers appropriate in light of their varying roles within the community. In the event of conflict between IT policies, this Appropriate Use Policy will prevail.

A. Appropriate Use. IT Systems may be used only for their authorized purposes -- that is, to support the educational, administrative, and other functions of Berean Christian High School. The particular purposes of any IT System as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the User.

B. Proper Authorization. Users are entitled to access only those elements of IT Systems that are consistent with their authorization.

C. Specific Proscriptions on Use. The following categories of use are inappropriate and prohibited:

1. **Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others**. Users must not deny or interfere with or attempt to deny or interfere with service to other Users in any way, including "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.
2. **Use that is inconsistent with Berean's non-profit status**. The school is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Systems for non-Berean purposes is generally prohibited, except if specifically authorized and permitted under School's conflict-of-interest, outside employment, and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers the School's educational, administrative, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.
3. **Use of IT Systems in a way that suggests the School's endorsement of any political candidate or ballot initiative is also prohibited**. Users must refrain from using IT Systems for the purpose of lobbying that connotes School involvement.
4. **Harassing or threatening use**. This category includes, for example, display of offensive, sexual material in the classroom and workplace as well as repeated unwelcome contacts with another.
5. **Use damaging the integrity of School or other IT Systems**. This category includes, but is not limited to, the following six activities:
   a) **Attempts to defeat system security**. Users must not defeat or attempt to defeat any IT System's security – for example, by "cracking" or guessing and applying the identification or password of another User, or compromising room locks or alarm systems. (This provision does not prohibit, however, Systems Administrators from using security scan programs within the scope of their Systems Authority.)
   b) **Unauthorized access or use**. The School recognizes the importance of preserving the privacy of Users and data stored in IT Systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. For example, a non-Berean organization or individual may not use non-public IT Systems without specific authorization. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-Berean organizations or individuals across the Berean network without specific authorization. Similarly, Users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept or attempt to intercept or access data communications not intended for that User, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.
   c) **Disguised use**. Users must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.
   d) **Distributing computer viruses**. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

e) **Modification or removal of data or equipment**. Without specific authorization, Users may not remove or modify any School-owned or administered equipment or data from IT Systems.

f) **Use of unauthorized devices.** Without specific authorization, Users must not physically or electrically attach any additional device (such as an external disk, printer, or video system) to IT Systems.

6. **Use in violation of law**. Illegal use of IT Systems -- that is, use in violation of civil or criminal law at the federal, state, or local levels -- is prohibited. Examples of such uses are promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing pornography; infringing copyrights; and making bomb threats.

   With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

7. **Use in violation of School contracts**. All use of IT Systems must be consistent with the School's contractual obligations, including limitations defined in software and other licensing agreements.

8. **Use in violation of School policy**. Use in violation of other School policies also violates this AUP. Relevant School policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment, as well as School, departmental, and work-unit policies and guidelines regarding incidental personal use of IT Systems.

9. **Use in violation of external data network policies**. Users must observe all applicable policies of external data networks when using such networks.

D. **Personal Account Responsibility**. Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Any User changes of password must follow guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users are presumed to be responsible for any activity carried out under their IT Systems accounts or posted on their personal web pages.

E. **Responsibility for Content**. Official School information may be published in a variety of electronic forms. The Certifying Authority under whose auspices the information is published is responsible for the content of the published document.

   Users also are able to publish information on IT Systems or over Berean's networks. Neither Berean nor individual Systems Administrators can screen such privately published material nor can they ensure its accuracy or assume any responsibility for its content. The School will treat any electronic publication provided on or over IT Systems that lacks a Certifying Authority as the private speech of an individual user.

F. **Personal Identification**. Upon request by a Systems Administrator or other School authority, Users must produce valid School identification.

II. Confidentiality and School Access

The School places a high value on privacy and recognizes its critical importance in an academic setting. There are nonetheless circumstances in which, following carefully prescribed processes, the School may determine that certain broad concerns outweigh the value of a User's expectation of privacy and warrant School access to relevant IT Systems without the consent of the User. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

A. **No Expectation of Privacy**. Users should have no expectation of privacy regarding communications or information sent or received through the School's email accounts, network, access to the Internet or School-provided resources, including student-issued iPads. BCHS reserves the right to access, review and monitor any electronic communication which utilizes any of Berean's IT Systems or networks, in accordance with applicable law, to ensure no misuse or violation of School policy or any law occurs.

   All data on student-issued iPads is considered the property of BCHS. The iPad and its data can be searched at any time with or without notice. Electronic documents, network usage, School email accounts, and all stored files, including any electronic messages that are created, sent, received or stored on the School's email system, network, iPads or computers, shall not be considered confidential and may be monitored at any time by designated School personnel to ensure appropriate use. BCHS complies fully with local, state or federal officials in any investigation concerning or relating with violations of computer crime laws.

POLICY SECTIONS (Continued)

B. **Process**. Consistent with the privacy interests of Users, School access without the consent of the User will occur only with the approval of the Principal (for faculty and student users), or his respective delegates, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public health and safety. The School, through the Systems Administrators, will log all instances of access without consent. Systems Administrators will also log any emergency entry within their control for subsequent review by the Principal or other appropriate school authority. A User will be notified of School access to relevant IT Systems without consent, pursuant to previous section A depending on the circumstance, such notification will occur before, during, or after the access, at the School's discretion.

C. **User access deactivations**. In addition to accessing the IT Systems, the School, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the User is suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, User services, or data. The Systems Administrator will attempt to notify the User of any such action.

D. **Use of security scanning systems**. By attaching privately owned personal computers or other IT resources to the School's network, Users consent to School use of scanning programs for security purposes on those resources while attached to the network.

E. **Logs**. Most IT Systems routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes.

F. **Encrypted material**. Encrypted files, documents, and messages may be accessed by the School under the above guidelines.

III. Safety and Security

A. **Limits of Filtering**. BCHS filters Internet traffic accessed via its IT Systems for the purposes of safeguarding students and staff from inappropriate and harmful content and for protection of devices and networks from malware. Nonetheless, despite the best efforts of the School, as no filtering and malware-protection methods are 100% effective, it remains possible that inappropriate and/or harmful content could be encountered by students, their parents/guardians, and staff while using BCHS IT systems or devices.

B. **Shared Responsibility for Safety.** Because of said limits of filtering, ensuring the safest technological experience possible requires cooperation of the entire School community. If, while using BCHS IT Systems, should student or staff personally encounter inappropriate material or suspected harmful content, or become aware of another party having encountered inappropriate or harmful content while using BCHS IT Systems, the student, and/or their parent/guardian, and/or BCHS staff shall immediately disengage from the content and then promptly report the suspected issue to a BCHS Systems Administrator or other BCHS Administrator so that, insofar as feasible, BCHS can take steps to block the inappropriate or harmful content from future access. Similarly, BCHS highly encourages parents/guardians to provide guidance to and supervise their student(s)/child(ren) when using technologies off-campus, whether using devices and networks provided by BCHS or using personal/family devices and networks, and to employ filtering and malware-protection strategies on home networks and devices.

C. **Hold Harmless Agreement**. This Policy shall be construed to contain the following agreement for students, their parents/guardians, and BCHS Staff: "In consideration of myself and/or my/our child/student participating in Berean Christian High School's educational and school program, I/we, and any legal representatives, heirs and assigns, hereby release, waive, and discharge Berean Christian High School, its officers, directors, employees, agents, and representatives from any and all liability for any and all loss or damage, and any claim for damages resulting therefrom, on account of exposure to inappropriate, offensive, and/or harmful content, including inadvertent disclosure of my/our child/student's personal information to a maleficent 3rd-party, by me or my/our child/student's attendance at and participation in Berean Christian High School's educational program and/or by using BCHS IT systems and/or devices, including any medical expenses, counseling expenses, injury, death, and/or damage to personal networks or devices from viruses, malware, or other malicious or harmful content. I/we agree to indemnify Berean Christian High School, its officers, directors, employees, agents, and representatives from any loss, liability, damage, or cost that may be incurred due to my own and/or my child/student's use of BCHS IT systems and/or devices, whether caused by negligence of Berean Christian High School, or otherwise. I fully understand, on my own behalf and/or on behalf of my child/student the risks associated with the aforementioned participation and assume any risk associated therewith.".

POLICY SECTIONS
(Continued)

IV. Enforcement Procedures

A. Complaints of Alleged Violations. An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint in accordance with established School Grievance Procedures. The individual is also encouraged to report the alleged violation to the Systems Authority, which must investigate the allegation and (if appropriate) refer the matter to School disciplinary and/or law enforcement authorities.

B. Reporting Observed Violations. If an individual has observed or otherwise is aware of a violation of this Policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Systems Authority, which must investigate the allegation and (if appropriate) refer the matter to School disciplinary and/or law enforcement authorities.

C. Disciplinary Procedures. Alleged violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the relevant Student or Faculty Handbook and other applicable materials. Students and staff members will be disciplined for violations of this Policy in accordance with the relevant disciplinary provisions set forth in handbooks covering their respective areas.

Systems Administrators may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority Systems Administrators are authorized to investigate alleged violations.

D. Penalties. Individuals found to have violated this Policy may be subject to penalties provided for in other School policies dealing with the underlying conduct. Violators may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the Systems Administrator.

E. Legal Liability for Unlawful Use. In addition to School discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

F. Appeals. Users found in violation of this Policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.