BETHLEHEM CHRISTIAN SCHOOL

INTERNET, SOFTWARE, COMPUTER AND NETWORK USER AGREEMENT POLICY

January 3, 2008

INTRODUCTION

Bethlehem Christian School (BCS) has developed this policy in order to maximize the benefits of our computer resources and minimize potential liabilities. The BCS computers, wired and wireless telephone systems, LAN and/or WiFi networks and all communications and information stored, transmitted, received, or contained in these systems, collectively referred to as 'BCS Systems', are the property of the Bethlehem Christian School Association and as such should be used for school-related purposes. A WiFi appliance is considered to include any electronic device that is wireless and/or mobile.

Please note that occasional personal use of BCS Systems is permissible if conceptually approved by your principal or his designated representative. This assumes that your personal use does not violate any of the basic tenets outlined in this policy, is not excessive and does not interfere with your instructinal performance.

All users of BCS Systems are obligated to use the Systems responsibly, ethically and lawfully. Note that this policy applies to Board Trustees, parents, students, teachers, staff and volunteers alike, who are all referred to in this policy, as 'Users'.

To ensure proper utilization of BCS Systems, we may occasionally monitor their use. Remember that any document that is created, stored, sent or received on BCS Systems is considered school property. BCS may review without prior notice, any material created, stored, sent or received on our network, our equipment or through the Internet by way of any BCS System.

Should a parent prefer that a student not have Internet access, use of the computers is possible for traditional purposes such as word processing, data management, and curriculum-based instruction.

PROHIBITED ACTIVITIES

Use of BCS Systems for any of the following activities is strictly PROHIBITED:

- Installing, downloading, sending, receiving, displaying, printing or otherwise disseminating material that is sexually explicit, pornographic, profane, obscene, harassing, fraudulent, racially offensive, defamatory, or otherwise unlawful, inappropriate or that may be offensive to others.

- Disseminating or storing commercial or personal advertisements, solicitations, promotions, destructive programs (that is viruses or self-replicating code) or any other unauthorized material, including but not limited to email spam.

- Changing, removing, or attempting to bypass BCS supplied, configured, or generated passwords.

- Wasting computer resources by spending time on creating, viewing, updating social websites, "surfing" the Internet and/or playing online games, engaging in online chat groups, printing multiple copies of documents or otherwise creating unnecessary network traffic.

- Installing and using personal software including but not limited to games.

  Please note…

  The use of some personal software is acceptable for school purposes only and must be approved by your principal and installed by the Network Administrator.

- Using or copying software in violation of any license agreement or copyright or the BCS software use policy as outlined in this policy document.

- Unless expressly authorized by your principal, or his designee, sending, transmitting or otherwise disseminating confidential data, or other confidential information of the school.
  - BCS recommends that all confidential email should be sent in an encrypted format to prevent unauthorized access.

- Violating any school rule, state or federal law.

- Searching the Internet in the classroom during a class activity with students observing.

Any student, parent, teacher, staff member or Board Trustee engaging in a prohibited activity will be subject to disciplinary action up to and including suspension "for cause". The disciplinary action taken will be determined by the seriousness of the offense.

PERMITTED ACTIVITIES

PASSWORDS AND SECURITY

User IDs and passwords are used for security and to establish accountability for activity on BCS Systems. All actions performed are the full responsibility of the person who has been assigned that user ID. Users are responsible for safeguarding their passwords and as such passwords should not be printed, stored online, or given to others. No user may access BCS Systems with another users' password or account without the express permission of that user and full knowledge of the campus principal. Users should provide another user with his or her password ONLY if the situation absolutely warrants it, AND THEN report to the Network Administrator for a reissuance of a new password.

BCS recommends that all users log off BCS computer systems when leaving their work areas for an extended period of time. If a user chooses to not to shut down, the user should not leave messages on the screen. A users' ability to connect to other computer systems, such as another computer through the network or via the Internet, does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the owners of those systems.

NOTIFY YOUR PRINCIPAL IMMEDIATELY IF UNAUTHORIZED USE OF USER IDS OR PASSWORDS IS DETECTED OR IF UNAUTHORIZED ACCESS TO ANY BCS SYSTEM IS DETECTED.

INTERNET USE

BCS provides users with access to the Internet to assist them in performing activities related to their work. Users must access the Internet only through the approved Internet firewall. The Internet can be a valuable source of information and research as well as an excellent means of communicating with other students, teachers, staff, board trustees, parents and businesses. Use of the Internet, however, must be tempered with common sense and good judgment. Searching the Internet as a method of classroom instruction, research, or project during class time with students observing is prohibited. Faculty and staff are directed to conduct appropriate research prior to classroom or project use. BCS is not responsible for material viewed or downloaded by users from the Internet. BCS has the right but not the duty to monitor all aspects of its computer system, including material downloaded or uploaded by users of the Internet. We recommend that all material downloaded from the Internet or from computers or networks that do not belong to BCS, be scanned for viruses before being placed onto BCS Systems.

SOFTWARE USE

BCS licenses the use of computer software from a variety of outside companies. BCS does not generally own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it except for backup purposes.

Client/server, network and web-based application software may be used only in accordance with the software license agreements.

1. Unauthorized software shall not be downloaded or uploaded over the Internet.

2. Software utilized in 'trial' mode shall be used strictly according to the vendor's trial period license provisions. Upon expiration of the trial period, the software must be deleted.

3. Users aware of any misuse of software or related documentation by another user shall notify their campus Principal or the Information Technology Director.

4. According to applicable copyright law, persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties, including fines and imprisonment. BCS does not allow the illegal duplication or use of software. Users who make, acquire, or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include suspension "for cause".

   NOTE: This suspension refers to removal of privileges from use of BCS Systems, as recommended by the campus Principal, and deemed appropriate by the BCS Head of School. The suspension would be assessed at a degree relative to the offense.

5. BCS requires that the machine-readable software media acquired as a result of a software purchase or through partner programs be held by a designated representative of the Information Technology Director.

   For software

   i. Supplied with equipment purchases, or
   ii. Purchased by BCS, or
   iii. Purchased by a user and reimbursed via expense vouchers, or
   iv. Provided to BCS as a gift,

   the media will be retained by BCS Administration, subsequent to the software being installed on the target PC. The Information Technology Director, or his designee, must approve in writing, any exceptions to this requirement.

For personally purchased and owned software installed in BCS assets, the owner must supply the Information Technology Department with a copy of the software media and a photocopy of the licensed media.

BCS reserves to the right to change, amend, remove, and add, etc content to this document as is deemed necessary.

STUDENT PROXY

BCS recognizes and acknowledges that students below the fifth grade may have difficult understanding and comprehending the intent and purpose of this document. Furthermore, such students may not recognize the potential dangers, troubles, and ramifications of engaging in activities that are not supported by this document. In such cases, BCS appoints by default of their position, the classroom teachers to act as proxy and on behalf of the students. In doing so, BCS expects the teachers will model and uphold the expectations expressed herein when using technology in the classroom for educational and non-educational use.
