Monte Vista Christian School

Information Technology

Students Use and Security Policy

Introduction

Computer information systems and networks are an integral part of the operation of Monte Vista Christian School. The school has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to:

- Maintain a safe and wholesome network environment for our students and staff.
- Safeguard the information contained within these systems.
- Protect the school's investment.
- Reduce business and legal risk.
- Protect the reputation of Monte Vista Christian School.

Violations

Failure to observe these guidelines may result in disciplinary action by the school depending upon the type and severity of the violation, whether it causes any liability or loss to the school, and/or the presence of any repeated violation(s).

Administration

The Director of Support Services is responsible for the administration of this policy.

Contents

The topics covered in this document include:

- **Policy responsibilities**
- **The Internet and e-mail**
- **Computer viruses, worms, and trojans**
- **Access controls and passwords**
- **Physical security**
- **Support**
- **Copyrights and license agreements**

Policy Responsibilities

General responsibilities pertaining to this policy are set forth in this section. Other sections list additional specific responsibilities.

Student responsibilities

All students must:

1. Ensure that they have read and understand the contents of this policy.
2. Comply with appropriate performance standards, control practices, and procedures as presented by their teachers.

The Internet and e-mail

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide.

Policy

Access to the Internet is provided by Monte Vista Christian School for the benefit of its staff and students. Internet users are able to connect to a variety of business and educational information resources around the world. Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all students are responsible and productive, and to protect the school's interests, the following guidelines have been established for using the Internet and e-mail.

Acceptable use

Students using the Internet are representing the school, and are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using a Web browser to obtain educational information from Web sites.
- Accessing databases for information as needed.
- Using e-mail for educational purposes.

Unacceptable use

Students must not use the Internet for purposes that are illegal, unethical, harmful to the school, or nonproductive. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Sending the same message to multiple people outside your immediate class.
- Conducting a personal business using school resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Streaming media that is readily available through other means.
- Accessing non-school related websites during normal school hours. i.e. Shopping on E-bay or accessing a personal email account.

Student responsibilities

Any student who uses the Internet or e-mail shall:

1. Ensure that all communications are for school related reasons and that they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that he/she places or sends over the Internet. All communications should have the sender's name attached.
3. Not transmit copyrighted materials without permission.

4. Not forward any virus or security bulletin to anyone with out express written permission of the IT Manager.
5. Not download any files that aren't required for a school related project.

Copyrights
Students using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. A copy of any such permission must be on file with the IT Manager. Failure to observe copyright or license agreements may result in disciplinary action by the school and/or legal action by the copyright owner.

Monitoring
All messages created, sent, or retrieved over the Internet are the property of the school and may be regarded as public information. Monte Vista Christian School reserves the right to access the contents of any messages sent over its facilities if the school believes, in its sole judgment, that it has a legitimate need to do so. All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or receiver. This means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.

Computer viruses, worms, and trojans

Computer viruses are programs designed to make unauthorized changes to programs and data. A computer worm is a program that copies itself from one disk to another, or replicates to multiple computers through e-mail and may damage or compromise the security of each computer it infects. Computer trojans are programs that do not usually spread by themselves, instead requiring some action by a user to install. Once installed a trojan's primary function typically is to compromise the security of a computer and/or network.

It is important to know that:

- Computer viruses, worms, and trojans are much easier to prevent than to cure.
- Defenses against these threats include protecting against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

Student responsibilities

These directives apply to all students:

1. Students shall not knowingly introduce a computer virus/worm/trojan into school computers.
2. Students shall not load removable storage media, i.e. Diskettes, USB drives and CDR disks, of unknown origin.
3. Incoming removable storage media shall be scanned for viruses before it is read.
4. Any person who suspects that his/her workstation has been infected shall notify the teacher or dean immediately.

Access controls and passwords

The confidentiality and integrity of data stored on the school computer systems must be protected by access controls to ensure that only authorized persons have access. This access shall be restricted to only those areas that are appropriate to each person's duties or assignments.

Student responsibilities

Each student:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password.
2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords must not be recorded where they may be easily obtained.
3. Shall not leave any workstation logged in, or in any state not requiring a password to continue working, if absent from the workstation.
4. Should change their passwords to conform with the Password Policy posted on the MVC Help Desk.
5. Will be required to change their passwords on a periodic basis. The network will begin notification one week prior to the required change. A new password will be required whenever logging on with the default password. If the password is forgotten it will be reset to the default password.
6. Shall not knowingly and without permission disrupt or cause disruption of any computer services, or attempt to access any unauthorized area, within or outside of the Monte Vista Christian School network.
7. Shall not knowingly and without permission attempt to obtain confidential network security information including but not limited to passwords, IP addresses or data packets.

Physical security

It is school policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Student responsibilities

The directives below apply to all students:

1. All files created by a student should be stored in their MyNetworkFiles, or Classes network files shares. This will ensure your files are backed up and accessible from any computer attached to the network. *(The IT Department is not responsible for the backup or recovery of files stored on a workstation or laptop.)*
2. No food or drink should be consumed or placed in the vicinity of any computer or associated component.
3. Since the IT Department is responsible for all equipment installations, disconnections, modifications, and relocations, no unauthorized persons are to perform these activities. This does not apply to temporary moves of notebook computers for which an initial connection has been set up by the IT Department.
4. Students shall not take shared portable equipment off campus.
5. Students should exercise care to safeguard the valuable electronic equipment they are assigned to use. Those who neglect this duty may be accountable for any loss or damage that results.
6. At no time may a student connect a computer to the network unless properly configured by the IT Department and approved by the IT Manager.
7. In order to ensure reliability, security and uniformity of support students should not attempt to change any settings relating to the desktop or folder options.
8. Due to a limited amount of disk space both on the primary and backup files servers, disk quotas have been implemented. Please do not store files that are not directly related to your classes needs on server based file shares. Locations are available for transferring large files to read/write CD’s. If you feel more storage space is needed, contact your teacher.

Support

The highly technical nature of computer networks and associated equipment may occasionally result in the need for support by the IT Department.

The following guidelines apply to support for all computer equipment on campus:

- In order to receive support, all equipment must be owned by the school and approved by the IT Manager for serviceability.
- Ink jet printers are difficult to maintain and expensive to operate. As such, please refrain from using or requesting them. A variety of network printers are available. If multiple copies are needed please use a copier.

To ensure that a verbal request is not overlooked and that fairness is maintained for all, please use the procedure as outlined below to obtained support.

Student responsibilities

Students should observe the following order for obtaining support:

1. Check the online Help Desk, http://mvcs.org/help.
2. Notify the staff member or teacher responsible for overseeing your activity.

Copyrights and license agreements

It is Monte Vista Christian School's policy to comply with all laws regarding intellectual property.

Monte Vista Christian School and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U.S. Code) and all proprietary software license agreements. Noncompliance can expose Monte Vista Christian School and the responsible student or staff member to civil and/or criminal penalties.

This directive applies to all software that is owned by Monte Vista Christian School, licensed to Monte Vista Christian School, or developed using Monte Vista Christian School resources by staff, students or vendors.

Civil penalties

Violations of copyright law expose the school and the responsible student or staff member to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines up to $100,000 for each illegal copy

Criminal penalties

Violations of copyright law that are committed "willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b))," expose the school and the student or staff member responsible to the following criminal penalties:

- Fines up to $250,000 for each illegal copy
- Jail terms of up to five years

Student responsibilities

Students shall not:

1. Install software unless authorized by the IT Manager. Licenses for all software must be on file with the IT Department.
2. Copy software unless authorized by the IT Manager.
3. Download software, for use on school computers, unless authorized by the IT Manager.

Acknowledgment of Information Technology Use and Security Policy

This form is used to acknowledge receipt of, and compliance with, the Monte Vista Christian School Information Technology Use and Security Policy. It must be signed and returned to the IT Manager or EdTech Director.

Procedure

Complete the following steps:

1. Read the Information Security Policy.
2. Sign and date in the spaces provided below.
3. Return this page only to the IT Manager or EdTech Director.
4. Failure to return this signed form will result in loss of network privileges.

Signature

By signing below, I agree to the following terms:

i. I have received and read a copy of the "Student IT Use and Security Policy" and understand and abide by the same;

ii. I understand and agree that any computers, software, and storage media provided to me by the school may contain proprietary and confidential information about Monte Vista Christian School and its teachers or its students, and that this is and remains the property of the school at all times;

iii. I agree that I shall not copy, duplicate (except for backup purposes as part of my studies here at Monte Vista Christian School), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;

Student signature: ____________________________________

Student (please print): ______________________________________

Grade: _______________________________________

Parent / Guardian signature: ____________________________________

Parent / Guardian (please print): ______________________________________

Date: ____