Technology Acceptable Usage Policy

St.Vincent Ferrer High School Technology Acceptable Usage Policy

INTRODUCTION:

To ensure that students receive a quality education and that employees are able to work in a professional and intellectually stimulating environment, it is the policy of the St.Vincent Ferrer High School to provide all students and employees with access to a variety of technology resources.

The creation of a large and varied technology environment demands that technology usage be conducted in legally and ethically appropriate ways, consistent with the Mission Statement and instructional goals of the St.Vincent Ferrer High School

Thus, it is the intention of the St.Vincent Ferrer High School that all technology resources will be used in accordance with all school system policies and procedures as well as local, state, and federal laws and/or guidelines governing the usage of technology and its component parts. Additionally, it is implied that all students and employees of the St.Vincent Ferrer High School will use the provided technology resources so as not to waste them, abuse them, interfere with or cause harm to other individuals, institutions, or companies.

The administrator of the school will be responsible for establishing specific practices to enforce this policy at St.Vincent Ferrer High School

All St.Vincent Ferrer High School technology resources, regardless of purchase date, location, or fund, are subject to this policy.

Any questions about this policy, its interpretation, or specific circumstance shall be directed to the Principal and Network Administrator, before proceeding.

Violators of this policy will be handled in a manner consistent with comparable situations requiring disciplinary and/or legal action.

POLICY STATEMENT:

The primary goal of the technology environment is to support the educational and instructional endeavors of students and employees of St.Vincent Ferrer High School. Use of any and all technology resources is a privilege and not a right.

I. ACCESS:

A. The use of all St.Vincent Ferrer High School technology resources is a privilege, not a right, and inappropriate or suspected inappropriate use will result in a cancellation of those privileges pending investigation.

B. Individuals may use only accounts, files, software, and technology resources that are assigned to him/her.

C. Individuals may not attempt to log in to the network by using another person's account and/or password or allow someone to use his/her password to access the network, e-mail, or the Internet.

D. Individuals must take all reasonable precautions to prevent unauthorized access to accounts and data or any other unauthorized usage within and outside the St.Vincent Ferrer High School.

E. Individuals identified as a security risk may be denied access.

F. Any use of technology resources that reduces the efficiency of use for other will be considered a violation of this policy.

G. Individuals must not attempt to disrupt any computer services or data by spreading viruses, spamming or by any other means.

H. Individuals must not attempt to modify technology resources, utilities, and configurations, or change the restrictions associated with his/her accounts, or attempts to breach any technology resources security system, either with or without malicious intent.

I. School administrators and Network Administrator will determine when inappropriate use has occurred and they have the right to deny, revoke, or suspend specific user accounts.

II. PRIVACY:

A. To maintain network integrity and to insure that the network is being used responsibly, the Network Administrator reserves the right to review files and network communications.

B. Users should not expect that files stored on the St.Vincent Ferrer High School'S network will always be private.

C. Because communications on the Internet are, often, public in nature, all users should be careful to maintain appropriate and responsible communications.

D. St.Vincent Ferrer High School cannot guarantee the privacy, security, or confidentiality of any information sent or received via the Internet.

E. Users should be aware that the technology staff routinely monitors and performs maintenance on fileservers, e-mail, workstations, the Internet, user accounts, telephones, and telephone systems. During these procedures, it may be necessary to review e-mail and/or files stored on the network.

F. Users are encouraged to avoid storing personal and/or private information/data on the schools technology resources.

G. The Network Administrator staff does perform routine backups. However, all users are responsible for storage of any critical files and/or data.

H. Student records, media center collections, and accounting information should be backed up to disk.

III. COPYRIGHT:

A. Illegal copies of software may not be created or used on school equipment.

B. Any questions about copyright provisions should be directed to the Network Administrator.

C. Copyright is implied for all information (text, data, and graphics) published on

the Internet. Web page authors will be held responsible for the contents of their

pages. Do not "borrow" icons or graphics from other pages without documented permission.

D. Duplication of any copyrighted software is prohibited unless specifically allowed for in the

License agreement and then, should occur only under the supervision and direction of the

appropriate administrator.

E. A backup copy of all purchased software programs should be made and, thus, become the

working copy.

F. All original copies of software programs, including those purchased with departmental

funds, will be stored in a secure place.

G. For security and insurance purposes, the Network Administrator should be the only person with access to original software disks at a given school location with the exception of CD-ROMs. System-wide software originals should be housed at the Network Administrator's office.

H. If a single copy of given software package is purchased, it may only be used on one computer at a time. Multiple loading or "loading the contents of one disk onto multiple computers," is NOT allowed.

I. If more than one copy of a software package is needed, a site license, lab pack, or network version must be purchased. The Network Administrator and the person requesting the Software will be responsible for determining how many copies should be purchased.

J. Either the Network Administrator or Principal in each school is authorized to sign license agreements for a school within the system. Copies of any system-wide license agreements must be signed by the Network Administrator and distributed to all schools that will use the software.

K. The Technology staff is responsible for installation and approval of all software in use on the local area network and/or individual workstations within the St.Vincent Ferrer High School.

L. Users should not purchase/download software/data without consulting the administrator.

IV. ELECTRONIC MAIL:

A. St.Vincent Ferrer High School provides access to electronic mail for all employees, class accounts upon request, and, on a limited basis, for students.

B. Access to e-mail is for employee, class, and/or student use in any educational and instructional business that they may conduct.

C. Personal use of electronic mail is permitted as long as it does not violate St.Vincent Ferrer High School policy and/or adversely affect others or the speed of the network.

D. Electronic mail should reflect professional standards at all time.

E. St.Vincent Ferrer High School e-mail accounts may not be used for political or personal gain.

F. St.Vincent Ferrer High School e-mail accounts may not be used to attempt or send anonymous messages.

G. St.Vincent Ferrer High School e-mail accounts may not be used for sending mass e-mails.

H. In most circumstances, St.Vincent Ferrer High School e-mail accounts should not be used for posting or forwarding other user's personal communication without the author's consent.

V. INTERNET:

A. The intent of the St.Vincent Ferrer High School is to provide access to resources available via the Internet with the understanding that faculty, staff, and students will access and use information that is appropriate for his/her various curricula.

B. All school rules and guidelines for appropriate technology usage shall apply to usage of the Internet.

C. Teachers should screen all Internet resources that will be used in the classroom prior to their introduction.

D. Students will gain access to the Internet by agreeing to conduct themselves in a considerate and responsible manner and by providing written permission from their parents.

E. Students will be allowed to conduct independent research on the Internet upon the receipt of the appropriate permission forms.

F. Students that are allowed independent access to the Internet will have the capability of accessing material that has not been screened.

VI. INTERNET FILTERING:

A. Internet access for all users is filtered, through one central point, by URL and IP address.

B. Internet searches are filtered by keyword.

C. URLs and IP addresses may be added to or deleted from the filtered list by the Network office.

VII. WEB PUBLISHING:

A. St.Vincent Ferrer High School server cannot be used for profit or commercial purposes.

B. All home pages will be reviewed by the Network Administrator before being added to the St.Vincent Ferrer High School World Wide Web Server.

C. Home pages may only be placed on the Web server by the Network Administrator.

D. All pages posted on the St.Vincent Ferrer High School web server must be written with an approved editor.

E. Each posted page must include: the school location, date of last update, and an e-mail address.

F. All posted work must be of publishable quality with regard to spelling, usage, and mechanics.

G. All web page authors are responsible for the maintenance of their own pages.

H. All links should be checked regularly to make sure they are current and working.

I. Pages that are not updated in a timely fashion; that contain inaccurate or inappropriate information; or contain links that do not work should be removed

J. Unfinished pages will not be posted until they are fully functional.

K. Pictures and other personally identifiable information should only be used with permission in writing from the parent/guardian of the student involved. No full names should be used-only first name, last initial. No written permission is required for in-school broadcasts (i.e. morning news, announcements, class profiles, etc.)

L. Student posting of personal information of any kind is prohibited. Personal information includes: home and/or school address, work address, home and/or school phone numbers, full name, social security number, etc.

M. No written permission is required to list faculty/staff and their school contact information (phone extension, e-mail address, etc.)

N. Infringement of copyright laws, obscene, harassing or threatening materials on web sites are against the law and are subject to prosecution.

O. Students can't record any lectures,teachers,students and school environment without prior written permission. Recording lectures will constitute intellectual property violation. All the above mentioned violation can lead to detention and or suspension.

VIII. EXAMPLES OF INAPPROPRIATE USE OF RESOURCES:

The following activities are examples of inappropriate activities for St.Vincent Ferrer High School' network, e-mail system, or the Internet. This list is not all-inclusive. Anything that would be considered inappropriate in "paper form" is also considered inappropriate in electronic form.

A. Using another user's password or attempting to find out what another user's password is.

B. Sharing your own password

C. Trespassing in another user's files, folders, home directory, or work

D. Saving information on ANY network drive or directory other than your Personal home directory OR a teacher specified and approved location. E. Downloading, installing, or copying software of any kind onto a workstation, your home directory, or any network drive.

F. Harassing, insulting, or attacking others via technology resources G. Damaging computers, computer systems, or computer networks (this includes changing workstation configurations such as screen savers, backgrounds, printers, BIOS information, preset passwords, etc.).

H. Intentionally wasting limited resources such as disk space and printing capacity.

I. Accessing inappropriate web sites (sites containing information that is violent, illegal, satanic, sexual, etc.)

J. Sending, displaying, or downloading offensive messages or pictures

K. Using obscene, racist, profane, discriminatory, threatening, or inflammatory language. Participating in on-line chat rooms without the permission/supervision of an adult staff member is prohibited.

M. Posting any false or damaging information about other people, the school system, or other organizations

N. Posting of any personal information about another person without his/her written consent.

O. Broadcasting network messages and/or participating in sending/perpetuating chain letters

P. Violating copyright laws

Q. Plagiarism of materials that are found on the Internet

R. Use of technology resources to create illegal.

S. Use of any St.Vincent Ferrer High School Technology resource for personal gain, commercial or political purpose.

To Parents:

The Internet also contains pornographic material, Web sites run by hate groups, and information on how to commit crimes. To prevent this information from entering our schools, we use an Internet filtering program. This program has a database of pornographic and other objectionable Web sites. We have configured the filtering program to block access to these Web sites.

Although the filtering program's database is updated frequently, there is always the possibility that a new pornographic or hate site will appear that has not been picked up by the program. For that reason, our teachers, librarians, and other staff members also monitor and supervise students' Internet access. Records of Internet access are also stored in computer log files, which we monitor periodically. These efforts help students learn how to use the Internet responsibly and avoid unsuitable sites. *Students who deliberately attempt to access pornographic and other blocked sites are subject to disciplinary procedures.*

Although our filtering software and monitoring efforts are designed to make the Internet an educational and safe experience, they cannot completely eliminate the risk that students will be able to access inappropriate material. **Therefore, parents may choose to opt their children out of accessing the Internet at school.**