Summer 1999

A Model Procedure for Monitoring Student on the Internet at Cashmere High School

Trevor Kert

A MODEL PROCEDURE FOR MONITORING

STUDENTS ON THE INTERNET

AT CASHMERE HIGH SCHOOL

by

Trevor Kert

July, 1999

The purpose of this project was to develop a model procedure for monitoring students on the Internet at Cashmere High School, Cashmere, Washington. To achieve this purpose, current research, literature, software, and acceptable use policies concerned with educational Internet usage were reviewed. Additionally, specific policies, agreements, and forms were adapted and developed to meet the needs of the Cashmere High School community.

ACKNOWLEDGEMENTS

This project is dedicated to my wife, Holly, and my family for their faithful support and encouragement throughout the entirety of this Master's Degree program.

The writer would also like to express his appreciation to Dr. Jack McPherson for his continued support, assistance, and invaluable advice in preparing this paper and during my complete course of study. In addition, I would also like to thank Dr. Steven Schmitz and Dr. Frank Carlson for their instruction and for their participation as members of my committee.

Finally, the writer would like to reflect any success to his Lord and Savior, Jesus Christ, through whom all things are possible!

TABLE OF CONTENTS

CHAPTER ONE

BACKGROUND OF THE PROJECT

Introduction

> The extremes of school Internet sentiment range from those who think it is an evil fad that should be banished to those who think it should be freely available to all with no restrictions whatsoever. Neither extreme is reasonable in the school setting. It is the prevailing belief of educational technology leaders that the Internet will continue to grow as a valuable and necessary communication system, to the benefit of educators and students alike. Ultimately, it is not a matter of whether schools access the Internet; rather, it is a matter of how schools serve and supervise students in learning the proper ways to use the Internet (Wilkinson, 1998).

As illustrated by Van Wilkinson in the above statement, differing views of the Internet and its educational use have been expressed. However, it is of great importance that schools monitor Internet usage as students use this vast technological tool. As more and more schools obtain the Internet, the problem of access to inappropriate material surfaces. Without knowledge of how to protect both the students and school district, serious problems can be just a few mouse clicks away.

According to an article in Curriculum Review (1996) students and teachers, alike, have explored the Web on a daily basis but so far, few districts have instituted a policy regarding the use of the Internet at school. In the words of President Clinton, "it is folly to think that we should sit idly by when a child who is a computer whiz may be exposed to things on that computer which in some ways are more powerful, more raw, and more inappropriate than those from which we protect them when they walk in a 7-11" (Diamond and Bates, 1995).

A course of action has been needed to guide a school district entering the world of cyberspace through the many pitfalls of inappropriate sites. The benefits of this incredible information superhighway can only be realized in a protected and monitored environment (Curriculum Review, 1996).

Purpose of the Project

The purpose of this project was to develop a model procedure for monitoring students on the Internet at Cashmere High School, Cashmere, Washington. To achieve this purpose, current research, literature, software, and acceptable use policies concerned with educational Internet usage were reviewed. Additionally, specific policies, agreements, and forms were adapted and developed to meet the needs of the Cashmere High School community.

Limitations of the Project

For purposes of this project, it was necessary to establish the following limitations:

1. Scope: The Internet acceptable usage policies and procedures were developed for use by the students, staff, and administration of Cashmere High School, Cashmere School District #504, Cashmere, Washington.
2. Research: The literature and software reviewed in Chapter 2 was essentially limited to research current within the last three (3) years. Additionally, selected school districts were contacted and invited to submit information regarding Internet usage policies unique to their individual programs.

3. Participants: Cashmere School District employees who assisted the writer, Trevor Kert, in planning and implementing the project included members of the Vocational department including: marketing education instructor, the Cashmere School District vocational director, the vocational guidance counselor, the Cashmere High School principal, and the Cashmere School District superintendent.
4. Time: This project focused on the school year 1998-99, to be implemented in the school year 1999-2000.

Definition of Terms

Significant terms used in the context of this study have been defined as follows:

1. Browser: a program that lets you view and explore information on the World Wide Web. (Marangraphics, 1997)
2. Communications Decency Act: Struck down in July 1997, this law was intended to ban the distribution via on-line communications to minors of "indecent" or "patently offensive" material and provide consequences for offenders. (Gruenwald, 1998)
3. Filter file: a file listing Web pages, newsgroups and other Net sites devoted to sex, drugs, racism, violence or other illegal, adult-oriented or potentially offensive activities. (Curtis, 1996)
4. Flamers: hostile and angry individuals, sexual predators, hard- and soft-core pornographers. (Frazier, 1995)
5. Gopher: an online menu system used to make searches easier. (Diamond and Bates, 1995)

6. IAUP: acronym for Internet Acceptable Use Policy which is used to outline the appropriate procedures that must be followed for appropriate educational Internet usage. (Belcer, 1996)
7. Internet: an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. (Marker, 1996)
8. Internet (legal definition): The global information system that is logically linked together by a globally unique address space base on the Internet Protocol (IP), or its subsequent extensions; and is able to support communications using the Transmission Control/Internet Protocol (TCP/IP) suite, or its subsequent extensions; and provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein. (California Business and Professions Code, Section 17738)
9. Web site: a collection of Web pages maintained by a college, university, government agency, company or individual. (Marangraphics, 1997)

CHAPTER TWO

REVIEW OF RELATED LITERATURE AND INFORMATION OBTAINED FROM SELECTED SOURCES

Introduction

The review of research and literature summarized in Chapter II has been organized to address:

1. The Internet: An Integral Part of Information Literacy in Schools
2. Case Law, Legislation, Censorship and Internet Implications
3. Software Filters
4. Summary of Related Information Obtained From Selected Sources
5. Summary

Data, current within the past four (4) years, was identified through an Educational Resources Information Center (ERIC) computer search. Various other online and print resources were used to conduct research.

The Internet: An Integral Part of Information Literacy in Schools

It has been the prevailing belief of educational technology leaders that the Internet will continue to grow as a valuable and necessary communications system, to the benefit of educators and students alike (Wilkinson, 1998). This sentiment was also shared by the Clinton Administration. In 1997, President Clinton set a lofty goal to connect all of America's school to the Internet by the twenty-first century (Lasica, 1997). According to Marker (1996) the question is no longer whether or not schools will connect to the Internet, but when.

Perhaps another reason the Internet has become such a powerful tool is due to the vast number of users who have had access. It has been estimated that more than 57 million people in over a 150 countries throughout the world use the Internet (Whitehead and Maran, 1997). Likewise, the Education Department estimated that more than half of the country's public schools have had access to the Internet (Riechmann, 1996). It has been noted from the wide spread use that the Internet is here to stay and has continued to become a valuable tool in education (Riechmann, 1996).

Curtis (1996), while citing the obvious value of the Internet as an incredible information resource, has cautioned Internet users of its offensive and potentially dangerous side. Risque and extremist material has run rampant online and this material is not appropriate for the educational setting. Curtis stated:

> The Internet can include pictures and text about everything from bizarre fetishes to prostitution to pedophilia-material that would shock many adults, let alone their children. And the nastiness does not stop there: violence, hate literature, cult information and drug lore have also seeped onto the Net and its cyberspace sibling, the World Wide Web.

According to Gruenwald (1998), these sites have been all to easy to find for curious minds. By typing a word such as "sex" on an Internet search engine, such as Yahoo, surfers will see numerous listings for sites advertising everything from "beautiful women. . .free photos" to the "best live sex shows".

Gruenwald (1998) also stated that even students who have attempted to avoid the many types of inappropriate materials available on the Internet are not always able to do so without having this material shoved in their faces. When searching for information on topics such as "animals" or "cheerleading,"

pornographic sites can be brought up by the student inadvertently (Gruenwald, 1998).

Not only are students not safe when they are simply surfing or looking around the Internet, but there is also the danger of those who are looking for them (Gruenwald, 1996). Child molesters have used the Internet to prey on children, establishing contact with a child through Internet chat rooms. Several cases have been investigated where children have been molested by an adult they first met while using the Internet (Gruenwald, 1998).

An incident very similar to what has been described above happened in 1998 at a nearby North Central Washington high school. A male student "met" a person in a chat room and corresponded several times over the Internet about developing a gay relationship. The school's Distributive Education Club of America (DECA) had a conference scheduled in the Seattle area so this particular student, who was a DECA member, arranged to meet this stranger at the hotel where the school club would be staying. While over in Seattle, the DECA advisor learned of the planned meeting and quickly involved hotel security to make sure the meeting would not take place. The dangerous situation was avoided and the matter was turned over to the administration upon the DECA club's return.

Diamond and Bates (1995) conducted a search for material that would be dangerous or hazardous to a school district. They started their search from the United State Department of Education's gopher server. In seven "hops" they reached "The School Stopper's Textbook," which gave direct instruction to students on how to blow up toilets, short circuit wiring, and "break into your school at night and burn it down." These are not exactly sites that would be appropriate to the education environment (Diamond and Bates, 1995).

Despite all of the necessary procedures that have been taken, Net-savy kids will always find a way to breach security measures (Diamond and Bates, 1995). "When there is question of inappropriate computer use or inappropriate material being viewed or downloaded from the Internet, the problem will eventually make it to the desks of the school administrators" said Diamond and Bates. For this reason, administrators need to be well versed in the Internet policies developed and implemented by their school districts. When problems arise over Internet usage, administrators will often be called on to explain or defend the policies used at their schools (Diamond and Bates, 1995).

Technology leaders must assure that students, teachers, parents, and board members have been made aware of the benefits and the possible hazards of the Internet (Frazier, 1995). Technology leaders must also remain current on the latest problems and solutions being developed on the ever changing Internet. Ultimately, however, school officials are responsible for monitoring students' behavior, determining when violations have occurred, and deciding whether consequences should be applied (Frazier, 1995).

Case Law, Legislation, Censorship and Internet Implications

Although the darker side of the Internet has been very real and readily apparent to anyone who wants to do a couple of quick searches for almost any topic, many people are opposed to any restrictions being placed on what students can or cannot view or even post on the Internet (Olsen and Meyer, 1996). A good example from the Bellevue School District demonstrated this point.

"The Unofficial Newport High School Home Page" was created by senior Paul K. Kim (Olsen and Meyer, 1996). This page satirized his peers' preoccupation with sex and sports and also contained links to sexually explicit resources. The principal was very upset when she learned of the page and withdrew her support for Paul as a National Merit Scholarship finalist and also wrote to the colleges Paul had applied to again withdrawing her recommendations. The American Civil Liberties Union became involved and brought suit against the district on Paul's behalf. The district lost the case, paid Paul $2000 for lost scholarship opportunities, and acknowledged that it had "no right to punish students who on their own time and with their own resources, exercise the right of free speech on the Internet" (Olsen and Meyer, 1996).

Opponents of Internet regulation argue that all students have constitutional rights (Peck and Symons, 1997). The Supreme Court ruling of 1969 which stated that students do not shed their constitutional rights to freedom of speech or freedom of expression is quickly noted when students' constitutional rights are endangered. This has not meant that school districts are free from Internet responsibility and have not been held liable for what a child encounters (Wilkinson, 1998).

In Iverson v. Muroc United School District (1995), a student was injured playing soccer in physical education class. The district claimed it could not be held responsible because public entities are not liable if a person engages in "hazardous recreational activity" on premises (Wilkinson, 1998). The court found differently because the soccer and physical education class were required during school hours so the student was allowed to prosecute. The indicated lesson was that districts could not have assumed that school Internet use was a "hazardous recreational activity," and districts could not have

taken the "use it at your own risk" position with regard to Internet usage (Wilkinson, 1998).

In a second court case cited by Wilkinson, Lucas v. Fresno United School District (1993), a student was hit by a dirt clod thrown by another student on campus. This district assumed under the doctrine of implied assumption of risk, there would be no district liability. Again the court disagreed citing that students are to be supervised and protected while on school district property. The indicated lesson in this case would have been that the Internet contains a risk component, so schools must supervise accordingly (Wilkinson, 1998).

In Brownell v. Los Angeles Unified School District (1994), the district won a suit involving a gang-related shooting that happened at the end of a school day. In this case, the court ruled that the school district was not the insurer of its students' safety. The court also ruled this way because steps had been taken for general safety and this shooting happened suddenly and without notice. The lesson stated by Wilkinson with regard to the Internet is that not all inappropriate material can be screened out, but schools must have taken precautionary steps to have minimized those occurrences (Wilkinson, 1998).

These court cases have proven that although students do not shed their constitutional rights to freedom of speech or expression, the school district is also responsible for the risks and hazards the Internet poses. Precautionary steps must be taken to protect schools from lawsuits that will occur as more and more students and schools use the Internet (Wilkinson, 1998).

Gruenwald (1998) explained the significance of the Communications Decency Act (1996) as the first attempt made by the United States' Congress to protect minors from pornography and other indecent material. However, this Act

was declared unconstitutional by the United States' Supreme Court in June 1997 because of infringement upon free speech rights.

The Clinton administration and the Internet industry have championed a ratings system for all Web sites to create a "family-friendly" environment in cyberspace (Lasica, 1997). "We need to encourage every Internet site, whether or not it has material harmful to minors, to rate its contents . . . to help ensure that our children do not end up in the red-light districts of cyberspace" said the President (Lasica, 1997).

Several Internet giants such as Netscape indicated that it would support ratings in its next browser. Other popular search engines such as Lycos, Excite and Yahoo! also pledged to ask for rating labels for all Web sites in their directories. Under this rating system, a user could choose a level between 0-4 for particular types of content. An example from the strong language area would be that of using the term "pig" for a police officer (Lasica, 1997). For using this term, the site would be given a rating of 3 for strong language. If a user adjusted a rating filter to screen out sites with strong language, those pages or sites would be blocked from the computer screen (Lasica, 1997).

Unfortunately this task has proved to be very difficult, with editors having to read and rate each story and deal with complaints by users who wonder why stories involving violence don't receive a strong enough rating. The rating system idea has been a very good one, but until it has become the law, it will remain largely unsuccessful (Lasica, 1997).

Savlov (1998) discussed the significance of recent legislation including the Internet School Filtering Act (1998) and the Communications Decency Act II (1998). The Internet School Filtering Act would require that school and public libraries install blocking and filtering software on any and all public-use

computers in an effort to shield minors from inappropriate material. This Act was sponsored by Dan Coats, a Republican from Indiana. Under this bill, commercial online distributors of material deemed harmful to minors would have been punished by up to six months in jail and a $50,000 fine. The Communications Decency Act II has been revised in order to appease a majority of those who feel this act is censorship in action. However, Savlov (1998) explained that the main thrust of the act has been to outlaw indecent or offensive material on the Internet.

Both the Internet Filtering Act and the Communications Decency Act II passed through the Senate. However, both the bill and the act are at the center of what many activists feel is a serious threat to online liberty. With such strong opposition, it could be a long time before this legislation would be in place. Schools allowing students to work on the wide open Internet cannot wait for these laws to be passed. Each district must take steps to protect the students, staff, and administration (Savlov, 1998).

Many people have forgotten that everyone has First Amendment rights, including children exploring the Internet, and according to Peck and Symons (1997), there are three First Amendment basics that must be recognized.

1. Obscenity is illegal and also a very narrow category of expression that the Supreme Court has said largely falls outside the First Amendment's protection.

2. Sexual expression, including nudity, that is merely indecent remains within First Amendment protection.

3. "Harmful to minors," another category, is essentially an obscenity standard using youngsters as the relevant yardstick. To be harmful to minors, speech must therefore be prurient, patently offensive, and without value for minors. Material that has substantial value for a significant minority of 17 year-olds cannot be considered

> harmful to minors. Thus, this category covers only a very narrow span of material. Forty-eight states have harmful-to-minors laws, many with exemptions for public libraries.

The First Amendment basics have made material that is obscene or harmful to minors illegal but in order to prosecute, specific state laws that define the illegal material and neutral due process hearings must be held (Peck and Symons, 1997). The pending legislation mentioned above would have helped prosecute those providing this obscene material to anyone surfing the Internet.

As soon as legislation that would filter or block indecent material on the Internet begins to make its way towards becoming law, The American Civil Liberties Union is quick to jump in charging that any crackdown on indecent material violates free speech (Curtis, 1996). In reference to the Communications Decency Act II, Legislative Consultant to the American Civil Liberties Union Ron Weich said, "the bill would criminalize constitutionally protected speech between adults and would have a chilling effect on a whole range of communications on the Internet; it (the bill) represents a serious threat to the First Amendment" (Savlov, 1998).

The Internet has become a vast information network with unlimited educational opportunities, but with these opportunities have come many dangers for students using the Internet and schools who have provided this access (Frazier, 1995). Recent court cases have revealed the fact that schools must protect students from the risk associated with the Internet and at the same time be very cautious of censoring what students are able to view on the Internet (Wilkinson, 1998). There have been pieces of legislation developed, but at this point, no real clear cut solution to help schools protect themselves and their students is available (Gruenwald, 1998).

The duty falls to each school and educators must ensure a protected environment for learning even in the classroom without walls (Pierson and Bitter, 1996). Software filters have become a possible solution to filtering out the inappropriate material and these should be used in conjunction with acceptable use guidelines and Internet acceptable use policies (Reichmann, 1996). "To ensure responsible use of the Internet, some schools are using commercial or in-house programs to block access to inappropriate material, says Linda Roberts, the Education Department's director of educational technology" (Reichmann, 1996). Administrators must be aware of potential problems and procedures in dealing with the Internet and Wilkinson (1998), has indicated that the best safeguard against Internet problems would be supervision that begins from the top down.

Software Filters

A brief description of a variety of software filtering solutions suggested by Pierson and Bitter (1996) that can limit inappropriate material and help provide a protected environment for the Internet, has been paraphrased below:

--SurfWatch-identifies over 10,000 potentially objectionable, sexually explicit or indecent materials on chat, gopher, newsgroup and Web sites. A monthly subscription updates the program with new sites. The program begins at computer start-up and requires no user modification.

--Netscape Nanny-monitors and blocks educator-identified unacceptable text in all applications running on the classroom computer and the Internet. Educators enter words, phrases, subjects and even personal information such as phone numbers into the administration dictionary. The program creates a log of their occurrences.

material or have an application shut down at a set limit of violations. The program screens incoming and outgoing text, scrutinized Internet sites, e-mail, chat lines, and offline applications, such as word processing.

--Cyber Patrol-a program for both Windows and Macintosh which prohibits access to 6000 different sites, divided into categories such as Sexual Acts/Text, Racist/Ethnic, and Violence/Profanity. Cyber Patrol also allows parents to restrict access to certain times of day, limit total time spent on-line per day or week, and control access to online providers and local applications such as games and personal financial managers.

--Net Blocker Plus-a program for both Windows and Macintosh which regulates conditions for student use of Internet sites, chat channels, newsgroups, and e-mail. Additionally, computer files and applications can be password protected.

--LinQ-a program for Macintosh or Windows consisting of hardware, software, and information service. School students or administrators make requests for information and after that information is researched and filtered by the LinQ team, it is delivered free of inappropriate language and content. The information is usually researched and transferred overnight.

--Net Nanny-a Windows program that comes with a dictionary of forbidden Web sites, newsgroups and chat rooms, to which parents can add or delete. Updates can be downloaded free of charge from the Net Nanny home page. As well as logging activity, it can also prevent a name, address, phone number or credit card number from being given out over the Internet. It has a two-way, real-time screening tool, which filters all conversations coming in and going out of the computer. For example, if someone in a chat room asks the child where he lives, the computer automatically shuts down.

--The Internet Filter-a Canadian program for Windows that comes with a fully configurable dictionary of sites and vocabulary, and logs all inappropriate access attempts by the child. Internet Filter also offers the option of alerting parents by sending an e-mail message to another computer, say, at the office when a child has attempted to access forbidden material.

--CYBERsitter-a Windows program featuring a filter file that lists Web pages, newsgroups and other Net sites devoted to sex, drugs, racism, violence or other illegal, adult-oriented or potentially offensive activities. When loaded and activated, the program prevents access to any of the forbidden sites, and it can alert parents to attempted access of those sites. CYBERsitter will also disallow certain words or phrases for use on the Internet or in e-mail, including the child's name, address, or phone number.

Summary of Related Information Obtained From Selected School Districts

Six (6) high schools around the state of Washington were contacted and invited to submit information descriptive of their computer and Internet policies. Specifically, information detailing the following issues was solicited:

1. High school Internet policy.
2. Steps followed to construct the Internet acceptable use policy.

High schools contacted included:

Manson High School
Manson, Washington

Bellevue High School
Bellevue, Washington

Wenatchee High School
Wenatchee, Washington

Bellingham High School
Bellingham, Washington

Brewster High School
Brewster, Washington

Pateros High School
Pateros, Washington

An analysis of information obtained from the above high schools revealed that five (5) characteristics were generally common to all Internet acceptable use policies. They included:

1. Network: All use of the computer system must be in support of education and research and consistent with the mission of the

Cashmere School District. The district reserves the right to prioritize use and access to the system.

2. Security: System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account number or password with another person or leave an open file unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.
3. Personal Security: Personal information such as addresses and telephone numbers should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher or other adult.
4. Copyright: The unauthorized installation, use, storage or distribution of copyrighted software or materials on Cashmere School District computers is prohibited.
5. General Use: No person shall have access to the system without having received appropriate training, and have signed and received approval in the form of an Individual User Release Form that must be on file with the district. Students under the age of 18 must have the approval of a parent or guardian.

An analysis of information obtained from the above high schools revealed that six (6) steps were used in the construction of several of the Internet acceptable use policies. These steps are very similar to six devised by Gerald Marker (1996) as a process for schools to follow who do not have any policy in place for the Internet. They included the following:

1. Enlist the aid of your computer coordinator, media director, librarian, principal, students, parents, and anyone else who has a policy interest in this area.

2. Collect examples of existing Internet acceptable use policies (IAUPs). Your state may have already endorsed a "suggested" version, and do not overlook the Internet itself.

3. Have one person draft the statement, then have it reviewed and revised by a committee that represents the many groups that have an interest in such a policy. Remember to include the school board attorney.

4. Try to convince the revision committee to take a least restrictive environment approach to the Internet. Enterprising students always seem to find a way around blocks and monitoring so do what you can to place the burden of responsible use on the student user.

5. Do what you can to give local meaning to the general terms that are used to describe appropriate resources and sites.

6. Encourage everyone on the committee to spend some time on the Internet. Let them see first hand what it is they are trying to regulate with their IAUP.

Summary

The research and literature summarized in Chapter 2 supported the following themes:

1. The Internet has continued to grow as a valuable and necessary tool of education but it has come with risks and hazards that must be minimized in the educational setting.
2. School districts are responsible for risks and hazards posed

by the Internet and must take the initiative to protect students while at the same time not impinging on their rights through unlawful censorship.

3. A variety of software solutions for limiting inappropriate material and providing a protected Internet environment are available and should be researched, purchased, and implemented at the district or building level.
4. Information obtained from selected high schools in Washington revealed the following commonalities:
    1. Characteristics of Internet acceptable use policies include the network, general security, personal security, copyright, and general use.
    2. A six (6) step process is often used by schools with no policy to follow in constructing a policy for their particular school.

CHAPTER THREE

PROCEDURES OF THE PROJECT

Introduction

The purpose of this project was to develop a model procedure for monitoring students on the Internet at Cashmere High School, Cashmere, Washington. To achieve this purpose, current research, literature, software, and acceptable use policies concerned with educational Internet usage were reviewed. Additionally, specific policies, agreements, and forms were adapted and developed to meet the needs of the Cashmere High School community.

Chapter 3 contains background information describing:

1. Need for the Project
2. Development of Support for the Project
3. Procedures of the Project
4. Planned Implementation and Assessment of the Project

Need for the Project

The need for this project was influenced by the following considerations:

1. The writer, Trevor Kert, a vocationally certified business education teacher, was assigned to teach computer and technology based classes in the Cashmere, Washington, School District from 1996-1999 and was seeking to prepare for the Internet accessibility that was to be available on 30 computer stations in the writer's home room.

2. After contacting selected business education teachers throughout Central Washington regarding the preparations necessary for safe and responsible student Internet usage, the writer determined there existed a need for:
    a. Internet usage agreement policies and procedures.
    b. Parent and student usage agreement forms.
    c. A software program to assist in filtering out inappropriate material.

3. Undertaking this study coincided with the writer's graduate studies at Central Washington University.

Development of Support for the Project

During the 1996-1997 school year, the writer engaged in working with fellow business education and marketing teacher, Chris Cloakey, on a proposal for the need, specifications, and funding for a new computer lab to better meet the needs of Cashmere High School students. During the 1997-1998 school year, a new computer lab with Internet capability was installed in the writer's home room.

The need to develop a model procedure for monitoring student Internet usage at Cashmere High School has emerged since 1998 as Internet connectivity was imminent. The following Cashmere School District employees individually and collectively encouraged and influenced the writer to undertake this project while contributing their expertise:

Cashmere High School District, Central Office Employees:

Mr. Joe Crowder - Superintendent
Mr. Mike Phillips - Business Manager

Cashmere High School Employees:

Mr. Sam Willsey - Principal
Mr. Tony Boyle - Assistant Principal
Mr. Jim Cockle - Vocational Director
Mr. Chris Cloakey - Business/ Marketing Instructor
Mrs. Holly Kert - English Instructor
Mrs. Becky Seidensticker-ESL Instructor

Cashmere High School was to have had Internet access in a computer lab with 30 computers available for use in vocational classes. The writer, Trevor Kert, was to be the main supervisor and teacher responsible for this computer lab. In the absence of an Internet acceptable use policy in the Cashmere School District, the writer felt the need and responsibility to develop a model procedure for monitoring student Internet usage at Cashmere High School to protect students, teachers, and administration from the occurrence of possible problems involved in Internet use.

Procedures of the Project

Additionally, the writer undertook the following procedures to develop a model procedure for monitoring student Internet usage at Cashmere High School.

1. Internet protection and filtering software from selected distributors was obtained and analyzed in order to make a

recommendation of software for the Cashmere School District to purchase upon receiving Internet access.

2. Software was to be downloaded off the Internet from selected locations and sites for the same purpose of testing each type of Internet filtering software.
3. Prices for the software that best fit the needs of Cashmere High School's students was obtained via the Internet, software catalogs, and software distributors.
4. The most complete software package with an appropriate site license price was to be recommended for purchase by Cashmere High School.
5. Information generally descriptive of Internet acceptable use policies and their construction was solicited from six (6) selected high schools, including:

Manson High School Manson, Washington	Bellevue High School Bellevue, Washington
Wenatchee High School Wenatchee, Washington	Bellingham High School Bellingham, Washington
Brewster High School Brewster, Washington	Pateros High School Pateros, Washington

6. Parent permission slips and student agreement forms were also requested, analyzed and adapted for Cashmere High School.

Planned Implementation and Assessment

The writer will present this model procedure for monitoring student Internet usage to a committee made up of Cashmere High School's principal, assistant principal, vocational director, and marketing education teacher to evaluate the findings of this Internet research project.

The committee will evaluate the different software products presented as well as cost and computer system requirements. The sample Internet acceptable use policies, parent permission slips, and student agreement forms will also be considered. The compilation of these samples adapted for Cashmere High School will be presented and critiqued by the committee.

Depending on when the T-1 line, a cable that will enable a large number of users to effectively use the Internet simultaneously, arrives at Cashmere High School and upon the approval of the above stated committee, this project will be implemented for the 1999-2000 or 2000-2001 school year. The recommended software portion of this project will be subject to the advancement of technology and availability of vocational funds.

Assessment of this Internet monitoring procedure will take place after students and staff have completed an introductory training of the acceptable use policy, software, expectations and user forms, and the procedure has been in place for a majority of the school year. Assessment will take place through the use of student, parent, and staff surveys, as well as, student behavior and performance in appropriate use of the Internet. Improvements and changes will be made after surveys are returned and data is gathered and analyzed.

CHAPTER FOUR

THE PROJECT

The model procedure for monitoring Internet usage designed for students and staff at Cashmere High School, which was the subject of this project, has been presented in Chapter Four, in four (4) units including:

Unit One- Parent Internet Awareness

Unit Two- Student Information

Unit Three-Filtering Software

Unit Four- Inappropriate Use Consequences

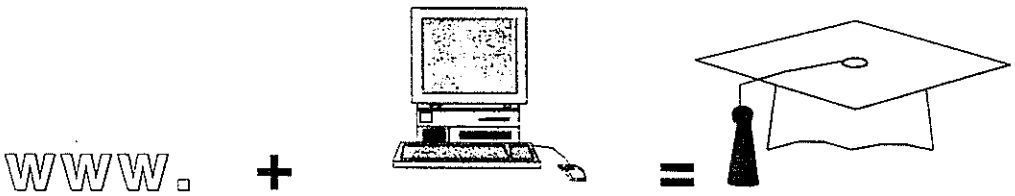
INTERNET USE

AT CASHMERE HIGH SCHOOL

INFORMATION FOR

THE

TWENTY-FIRST CENTURY



CASHMERE SCHOOL DISTRICT

CASHMERE HIGH SCHOOL TECHNOLOGY EDUCATION

Trevor Kert, Instructor

TABLE OF CONTENTS

INTERNET USE

AT CASHMERE HIGH SCHOOL

Unit One

Parent Internet Awareness

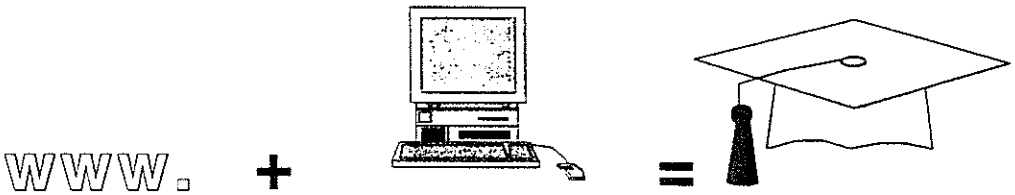


Table of Contents

Parent Internet Awareness

Parent Internet Awareness

Unit Overview

Students at Cashmere High School now have the opportunity to use the Internet in certain classes they take at the high school. In this unit, parents will learn about the opportunities their students have as well as the expectations and procedures that must be followed in order to take full advantage of those opportunities.

Internet Opportunities

Students will be able to:

- Research careers that match their individual skills, interests, and abilities.
- Visit educational web sites for information helpful for class projects.
- Register for an E-mail account (pending availability and class enrollment).
- Learn to navigate the World Wide Web.
- Access on-line materials such as periodicals and encyclopedias.
- Stay up-to-date on current events using various news sites.

Acceptable Use Policies

In order for students to be given the Internet opportunities listed above, parents and students must be familiar with and in agreement of Cashmere High School's acceptable use policies listed below.

Cashmere School District Acceptable Network Use Policies

Cashmere High School is implementing an electronic communications system (network) that will allow unprecedented opportunities for students, staff, and patrons to communicate, learn, access and publish information. It is believed that the resources available through this network and the skills that students will develop in using it, are of significant value in the learning process and in assuring their success in the future. These new opportunities also pose many new challenges including, but not limited to, access for all students, age level appropriateness of material, security, and cost of maintaining ever more elaborate systems. The district will endeavor to ensure that these concerns are appropriately addressed, but cannot ensure that problems will not arise.

By creating this network, Cashmere High School intends only to provide a means for educational activities and does not intend to create a first amendment forum for free expression purposes. The district dedicates the property comprising the network, and grants access to it by users only for the educational activities authorized under this policy and procedures and under the specific limitations contained therein.

The high school intends to provide training and procedures that encourage the widest possible access to electronic information systems and networks by students, staff, and patrons while establishing reasonable controls for the lawful, efficient and appropriate use and management of the system.

ACCEPTABLE USE GUIDELINES

Network

1. All use of the system must be in support of education and research and consistent with the mission of the Cashmere School District. The district reserves the right to prioritize use and access to the system.

2. Any use of the system must be in conformity to state and federal law and district policy. Use of the system for commercial solicitation is prohibited.

3. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.

4. No use of the system shall serve to disrupt the operation of the system by others; system components including hardware or software shall not be destroyed, modified or abused in any way.

5. Malicious use of the system to develop programs that harass other users or gain unauthorized access to any computer or computing system and/or damage the components of a computer or computing system is prohibited.

6. Users are responsible for the appropriateness and content of material they transmit or publish on the system. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors as expressly prohibited.

7. Use of the system to access, store, or distribute obscene or pornographic material is prohibited.

8. Subscriptions to mailing lists, bulletin boards, chat groups and commercial on-line services and other information services must be pre-approved by the district.

Security

9. System accounts are to be used only by the authorized owner of that particular account for the authorized purpose. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.

10. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorized access to the system.

11. Communications may not be encrypted so as to avoid security review.

12. Users should change passwords regularly and avoid easily guessed passwords.

Personal Security

13. Personal information such as addresses and telephone numbers should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher or other adult.

14. Students should never make appointments to meet people in person that they have contacted on the system without district and parent permission.

15. Students should notify their teacher or other adult whenever they come across information or messages that are dangerous, inappropriate, or make them feel uncomfortable.

Copyright

16. The unauthorized installation, use, storage or distribution of copyrighted software or materials on Cashmere School District computers is prohibited.

General Use

17. Diligent effort must be made to conserve system resources. For example, frequently delete E-mail and unused files.

18. No person shall have access to the system without having received appropriate training, and signed and received approval in the form of an Individual User Release Form. This IURF must be on file with the district. Students under the age of 18 must have the approval of a parent or guardian.

19. These regulations are not intended to preclude the supervised use of the system by students while under the direction of a teacher or other approved user acting in conformity with district policy and procedure. All student use is to be under the supervision of the teacher or other designated staff.

From time to time, the district will make a determination on whether specific uses of the system are consistent with the regulations stated above. Under prescribed circumstances the use by individuals other than students or staff may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the district. For security and administrative purposes, the district reserves the right to review system use and file content by authorized personnel. The district reserves the right to remove a user account on the system to prevent further unauthorized activity.

Violation of any of the conditions of use may be cause for disciplinary action.

Cashmere High School

Parent Information Letter

Internet and Electronic Mail Information

Your child has the opportunity to receive an electronic network account or access and needs your permission to do so. Among other advantages, your child will be able to communicate with other schools, colleges, organizations, and individuals around the world through Internet and other electronic information systems and networks. The Internet is a system which links smaller computer networks, creating a large and diverse network. Internet allows your child, through electronic mail (e-mail) and other means to reach out to many other people to share information, learn concepts, and research subjects. These are significant learning opportunities to prepare your child for the future.

With the educational opportunity also comes responsibility. It is important that you and your child read the enclosed informed consent forms, school district procures, and other material, and discuss it together. When your child is given an account and password to use on the computer, it is extremely important that the rules are followed. Inappropriate use will result in the loss of privilege to use the educational tool, and other disciplinary action if needed. Parents, remember that you are legally responsible for your child's actions.

Please stress to your child the importance of using only his or her account password, and of keeping it a secret from other students. Your child should never let anyone else use their password to access the network. Your child is responsible for any activity that happens in their account.

We have established procedures and rules regulating the materials that students may search for on the network. It is not possible for us to always provide direct supervision of all students. We encourage you to consider the potential for your child being exposed to inappropriate material in your decision of whether or not to sign the informed consent form.

If you have any questions, please contact the high school. If you want your child to have the opportunity to receive an Electronic Network account or access, please return the signed informed consent forms to us as soon as possible.

Sincerely,

Sam Willsey
High School Principal

Cashmere High School

Parent Signature Form

Internet and Electronic Mail Permission Form

Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply.

The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Parent permission is required. Access is a privilege - not a right. Access entails responsibility.

Individual users of the district computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with district standards and will honor the agreements they have signed. Beyond the clarification of such standards, the district is not responsible for restricting, monitoring, or controlling the communications of individuals utilizing the network.

Network storage areas may be treated like school lockers. Network administrators and/or teachers may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private. Within reason, freedom of speech and access to information will be honored.

The following are not permitted:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using another's password
- Trespassing in another's folders, work or files
- Employing the network for commercial purposes

As the parent or legal guardian of the student named below, I grant permission for my son or daughter to access networked computer services such as electronic mail and the Internet. I understand that individuals and families may be held liable for violations. I understand that some materials on the Internet may be objectionable, but I accept responsibility for guidance of Internet use - setting and conveying standards for my son or daughter to follow when selecting, sharing, or exploring information and media.

Parent Signature _____ Date _____

Name of Student _____

School _____ Grade _____

Soc. Sec.# _____ Birth Date _____ Street Address _____

Home Telephone _____

Cashmere High School

Parent Information Letter in Spanish

Internet and Electronic Mail Information

Su niño tiene la opportunidad de recibir un acceso o cuenta de red electônica y necesita su permiso para hacer esto. Entre otras ventajas, su niño serâ capaz para comunicarse con otras escuelas, colegios, organizaciones e individuos alrededor del mundo mediane Internet, y otras redes electrônicas y sistemas de informaciôn. Internet es un sitema que vincula las redes menores de computadora, creando una red diversa y grande. Internet permite que su niño, mediante el correo electrônico y los otros medios pueda alcanzar mucha otra gente para compartir informaciôn y conceptos. Estas oportunidad de aprendizaje son importantes para preparar a su hijo en el futuro.

Con esta oportunidad educativa tambiên vinen responsabilidades. Es importante que Ud. y su niño lean la forma de consentimiento adjunta, procedimientos de la escuela y el otro material, y discutirlo juntos. Cuando se le da una cuenta o contraseña para usar en la computadora, es sumamente importantne que las reglas se sigan. El uso impropio resultarâ en la pêrdida del privilegio para usar este medio educativo, y otra acciôn desciplinaria si es apropiada. Padres, recuerden que Uds. son legalmente responsables por las acciones de su niño.

Por favor hable con su niño acerca de la importancia de usar ûnicamente su cuenta o contraseña, y de guardar lo como un secreto para otros estudiates. Su niño no debera dejar nunca a otra persona usar su contraseña acceder a la red. Su niño es reposable por cualquier actividad que suceda en su cuenta.

Nosotros tenemos reglas y procedimentos establesidos que regulan las materia que los estudiantes pueden buscar en la red. No es pocible para nosotros proveer siempre supervisiôn directa a todos los estudiantes. Nosotros fomentamos a Ud. que considere la potencialidad de su niño siendo expuesto a la materia impropia es su decisiôn de si or no firmar la forma de concentimiento.

Si Ud. tiene cualquier pregunta por favor llame a los directores de la escuela. Si Ud. quiere que su niño tenga la oportunidad de recibir un acceso de Internet o cuenta de red, por favor regrese las formas fimadas de concentimiento a nosotros lo antes posible.

Sincerely,

Sam Willsey
Director de la Secundaria

INTERNET USE

AT CASHMERE HIGH SCHOOL

Unit Two

Student Information

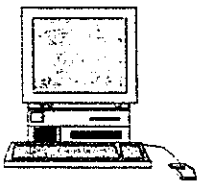
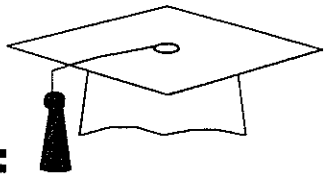
www. +  = 

Table of Contents

Student Information

Student Information

Unit Overview

Students at Cashmere High School now have the opportunity to use the Internet in certain classes they take at the high school. In this unit, students will learn about the opportunities they have as well as the expectations and procedures that must be followed in order to take full advantage of those opportunities.

Student Learning Objectives

Students will be able to:

- Research careers that match their individual skills, interests, and abilities.
- Visit educational web sites for information helpful for class projects.
- Register for an E-mail account (pending availability and class enrollment).
- Learn to navigate the World Wide Web.
- Access on-line materials such as periodicals and encyclopedias.
- Stay up-to-date on current events using various news sites.

In order to take advantage of the following privileges, the following Internet acceptable use guidelines must be understood. Students must also agree to abide by these guidelines by signing a student user form.

ACCEPTABLE USE GUIDELINES

Network

1. All use of the system must be in support of education and research and consistent with the mission of the Cashmere School District. The district reserves the right to prioritize use and access to the system.

2. Any use of the system must be in conformity with state and federal law and district policy. Use of the system for commercial solicitation is prohibited.

3. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.

4. No use of the system shall serve to disrupt the operation of the system by others; system components including hardware or software shall not be destroyed, modified or abused in any way.

5. Malicious use of the system to develop programs that harass other users or gain unauthorized access to any computer or computing system and/or damage the components of a computer or computing system is prohibited.

6. Users are responsible for the appropriateness and content of material they transmit or publish on the system. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors as expressly prohibited.

7. Use of the system to access, store, or distribute obscene or pornographic material is prohibited.

8. Subscriptions to mailing lists, bulletin boards, chat groups, and commercial on-line services and other information services must be pre-approved by the district.

Security

9. System accounts are to be used only by the authorized owner of that particular account for the authorized purpose. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.

10. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorized access to the system.

11. Communications may not be encrypted so as to avoid security review.

12. Users should change passwords regularly and avoid easily guessed passwords.

Personal Security

13. Personal information such as addresses and telephone numbers should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher or other adult.

14. Students should never make appointments to meet people in person that they have contacted on the system without district and parent permission.

15. Students should notify their teacher or other adult whenever they come across information or messages that are dangerous, inappropriate, or make them feel uncomfortable.

Copyright

16. The unauthorized installation, use, storage or distribution of copyrighted software or materials on Cashmere School District computers is prohibited.

General Use

17. Diligent effort must be made to conserve system resources. For example, frequently delete E-mail and unused files.

18. No person shall have access to the system without having received appropriate training, and signed and received approval in the form of an Individual User Release Form. This IURF must be on file with the district. Students under the age of 18 must have the approval of a parent or guardian.

19. These regulations are not intended to preclude the supervised use of the system by students while under the direction of a teacher or other approved user acting in conformity with district policy and procedure. All student use is to be under the supervision of the teacher or other designated staff.

From time to time, the district will make a determination on whether specific uses of the system are consistent with the regulations stated above. Under prescribed circumstances the use by individuals other than students or staff may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the district. For security and administrative purposes, the district reserves the right to review system use and file content by authorized personnel. The district reserves the right to remove a user account on the system to prevent further unauthorized activity.

Violation of any of the conditions of use may be cause for disciplinary action.

Cashmere High School

Student User Form

Internet and Electronic Mail Permission Form

Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply.

The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Parent permission is required. Access is a privilege - not a right. Access entails responsibility.

Individual users of the district computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with district standards and will honor the agreements they have signed. Beyond the clarification of such standards, the district is not responsible for restricting, monitoring, or controlling the communications of individuals utilizing the network.

Network storage areas may be treated like school lockers. Network administrators and/or teachers may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private. Within reason, freedom of speech and access to information will be honored.

The following are not permitted:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using another's password
- Trespassing in another's folders, work or files
- Employing the network for commercial purposes

I understand that some materials on the Internet may be objectionable and I accept responsibility for my use of the Internet when selecting, sharing, or exploring information and media. I agree to abide by Cashmere High School's Policy and Procedures for Electronic Information Systems and understand that I may be held liable for violations.

Printed Name _____ Date _____

Signature _____ Grade _____

Address_____ City/State/Zip _____

Home Telephone _____

*Students over eighteen do not need a parent's signature.

INTERNET USE

AT CASHMERE HIGH SCHOOL

Unit Three

Filtering Software

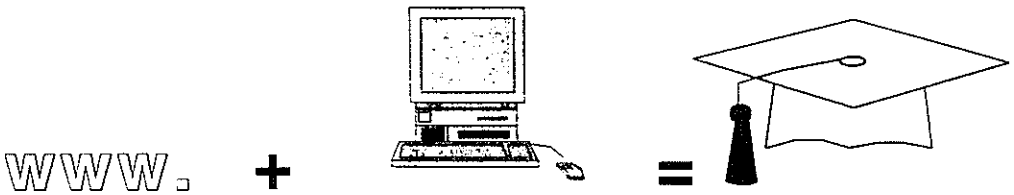


Table of Contents

Filtering Software

Filtering Software

Unit Overview

Along with Internet acceptable use guidelines and parent and student permission and user forms, filtering software will be implemented to help ensure a safe environment. In this unit, the purpose of this software is explained and the ways in which it will assist in providing a safe environment are described. Examples are also given so this software can be seen in action.

Purpose

The Internet has many benefits for use in schools. The sharing of resources and ideas, communicating with people in far off places, readily accessing reference materials, and the list goes on. But along with the benefits come the drawbacks of exposure to such things as hate mail, racism, pornography, bomb and drug formulas and unfortunately, this list also goes on.

Although parents and student have agreed these sites will be avoided and not accessed, removing as many chances and temptations on computer screens as well as noting what sites are accessed can only help. Filtering software can be used to limit the poor choices and many inappropriate solicitations available on the web. When students understand that where they travel in cyberspace can be retraced and monitored, this filtering software will help deter them from going to sites they shouldn't because of the accountability that this software will provide.

Description

This is where the filtering software Net Nanny can be used to act as an invisible monitor between the Internet and users at Cashmere High School. It will operate quietly in the background, carefully screening out user defined sites, words, phrases, and content that is determined as inappropriate for the high school setting. Net Nanny has many benefits listed below and can be use to filter and block sites, as well as, monitor other programs running on classroom computers.

Net Nanny Benefits

- Prevents students from giving out personal information such as their address, phone, or credit card numbers on the Internet.
- Provides users with free "can go" and "can't go" site lists to download into screening databases.
- Prevents user-definable words, phrases, personal information, Internet web sites, Internet news groups, and IRK chat rooms from being sent from, received by, or accessed by a student's computer.
- Masks inappropriate words, phrases, or language.
- Develops your own screening lists for web sites, words, phrases, personal information, newsgroups, and chatrooms.
- Event log which indicates computers start-up, and violation occurrences including dates and times.
- Operates with all major Online Providers and in e-mail and IRK.
- Screens all computer activity including Internet tools and other bulletin board services online, and any and all Windows or DOS applications.

Net Nanny has other convenient functions that can be detailed for the Cashmere High School community. Net Nanny can be told by teachers and administrators what should or should not be entered or received on school computers. The terminal action that should take place can also be chosen such as: log the hit, mask words on screen, give a warning, block access, or shutdown the application, or any combination of these choices.

Filtering and Blocking Options

Net Nanny allows you to filter and block:

- Internet web sites
- Newsgroups
- Chat channels
- Personal information
- Words and phrases

Program Monitor Options

Net Nanny can monitor any program on your student's computer including:

- E-mail programs such as Outlook, Pegasus, Eudora and others
- Chat programs such as MIRC, PIRCH and others
- Internet browsers including Internet Explorer and Netscape
- ICQ
- MS Word
- Notepad and Wordpad

Purchase Information

Computers must have the following system requirements in order to run the newest version of Net Nanny:

Hardware

- IBM personal computer or IBM compatible microcomputers
- Mouse or pointing device
- Hard Drive, minimum 4 megabytes available disk space
- Recommended processor of 486 or above

Operating System

- Microsoft Windows 3.1 (or later versions), Windows 95 or Windows 98
- Minimum 4 megabytes of random access memory (8 or more recommended)

Prices as of March 1999

Single User:	$39.95 plus $6.95 shipping
Educational Site Licenses:	$200 ($10 each with a minimum of 20) 10% discount after 200 units

Address

Net Nanny Limited
525 Seymour Street, Suite 108
Vancouver, BC V6B 3H7
Canada

Telephone: (604) 662-8522
Fax: (604) 662-8525

INTERNET USE

AT CASHMERE HIGH SCHOOL

Unit Four

Inappropriate Use Consequences

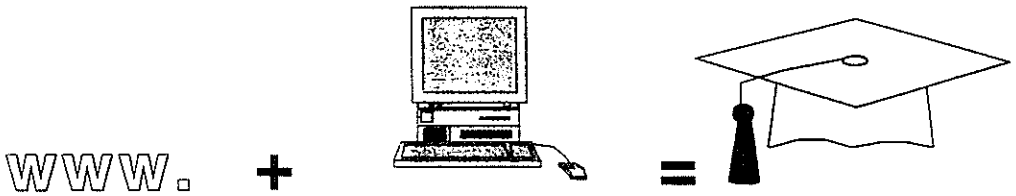


Table of Contents

Inappropriate Use Consequences

Inappropriate Use Consequences

Unit Overview

To promote a safe and comfortable environment for everyone using the Internet at Cashmere High School, consequences for inappropriate Internet use will be provided to those who violate their user agreement forms. In this unit, these consequences will be described and school handbook policy regarding inappropriate Internet use will also be defined.

Administrative Procedures

A safe and orderly school environment is essential for teaching and learning involving the Internet to take place. Students must adhere to a code of appropriate usage regarding the Internet, not only for their own benefit, but also for the benefit of others. This code is in effect during school hours, on school property, and during school related activities.

Students are responsible for their own actions and are held accountable for:

1. All rules and responsibilities within the Internet acceptable use policy.
2. The Cashmere School District Board of Directors policies concerning student conduct.
3. And other rules set forth by the Cashmere High School administration.

Students not adhering to any of the above will be subject to discipline, suspension, and/or expulsion.

Handbook Penalty Page

Cashmere High School will follow a progressive discipline policy when dealing with offenses related to inappropriate Internet usage. Below, four levels of discipline are listed. Students who accumulate multiple offenses at Level I or Level II will be considered for more serious consequences. The student who is suspended from school will be asked to have a parent or guardian conference with school authorities.

LEVEL I: 1-4 hours school service, Saturday School and/or parent conference.

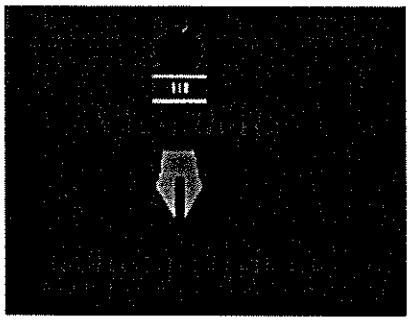
LEVEL II: Loss of Internet privileges with short term in-school or out-of-school suspension for up to ten (10) days. WAC 180-40-235.

LEVEL III: Long term suspension up to eighteen (18) weeks. WAC 180-40-260.

LEVEL IV: Expulsion in accordance with WAC 180-40-275.

For a number of minor policy infractions, the normal procedure for progressive discipline shall be Level I (other forms of corrective action may be used before a student arrives at Level I). The severity of an Internet use infraction will be determined by the administrators at Cashmere High School.

Appendices



Parent Letter:

Dear Parents:

Your child has the opportunity to receive an electronic network account or access, and needs your permission to do so. Among other advantages, your child will be able to communicate with other schools, colleges, organizations and individuals around the world through Internet and other electronic information systems and networks. Internet is a system which links smaller computer networks, creating a large and diverse network. Internet allows your child, through electronic mail (e-mail) and other means to reach out to many other people to share information, learn concepts and research subjects. These are significant learning opportunities to prepare your child for the future.

With this educational opportunity also comes responsibility. It is important that you and your child read the enclosed informed consent form, school district procedures and other material, and discuss it together. When your child is given an account and password to use on the computer, it is extremely important that the rules are followed. Inappropriate use will result in the loss of the privilege to use this educational tool, and other disciplinary action if appropriate. Parents, remember that you are legally responsible for your child's actions.

Please stress to your child the importance of using only his or her account password, and of keeping it a secret from other students. Your child should never let anyone else use their password to access the network. They are responsible for any activity that happens in their account.

In spite of our efforts to establish procedures and rules regulating the materials that students may search for on the network, please be aware that there is unacceptable and controversial material and communications on the Internet that your child could access. We cannot filter material posted on network-connected computers all over the world. You need to consider the risk of your child being exposed to inappropriate material in your decision of whether or not to sign the informed consent form.

If you have any questions please contact me at *telephone number*. Please return signed informed consent forms to us as soon as possible.

Sincerely,

WHS Home Page	WHS Departments	WHS Special Features	Educational Sites	Wenatchee Valley Events	News

Last modified 7 Jan 98

Bellingham Public Schools

You may copy this form.

Parent Permission Letter

Internet and Electronic Mail Permission Form

The Bellingham Public Schools

We are pleased to offer students of the Bellingham Public Schools access to the district computer network for electronic mail and the Internet. To gain access to e-mail and the Internet, all students under the age of 18 must obtain parental permission and must sign and return this form to the LIBRARY MEDIA SPECIALIST. Students 18 and over may sign their own forms.

Access to e-mail and the Internet will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with Internet users throughout the world. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the Bellingham Public Schools support and respect each family's right to decide whether or not to apply for access.

District Internet and E-Mail Rules

Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply.

The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Parent permission is required. Access is a privilege - not a right. Access entails responsibility.

Individual users of the district computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with district standards and will honor the agreements they have signed. Beyond the clarification of such standards, the district is not responsible for restricting, monitoring or controlling the communications of individuals utilizing the network.

Network storage areas may be treated like school lockers. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private.

Within reason, freedom of speech and access to information will be honored. During school, teachers of younger students will guide them toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television,

, radio and other potentially offensive media.

oard policy and procedures on student rights and responsibilities (3200), copies of able in school offices, the following are not permitted:

- ıg or displaying offensive messages or pictures
- g obscene language
- assing, insulting or attacking others
- amaging computers, computer systems or computer networks
- Violating copyright laws
- Using another's password
- Trespassing in another's folders, work or files
- Intentionally wasting limited resources
- Employing the network for commercial purposes

Violations may result in a loss of access as well as other disciplinary or legal action.

User Agreement and Parent Permission Form - 1995

As a user of the Bellingham Public Schools computer network, I hereby agree to comply with the above stated rules - communicating over the network in a reliable fashion while honoring all relevant laws and restrictions.

Student Signature _____

As the parent or legal guardian of the minor student signing above, I grant permission for my son or daughter to access networked computer services such as electronic mail and the Internet. I understand that individuals and families may be held liable for violations. I understand that some materials on the Internet may be objectionable, but I accept responsibility for guidance of Internet use - setting and conveying standards for my daughter or son to follow when selecting, sharing or exploring information and media.

Parent Signature _____ Date _____
Name of Student _____
School _____Grade _____
Soc. Sec.#_____ Birth Date _____ Street Address _____ Home Telephone _____
