Internet Safety Plan

Danville Public Schools

2011-2012

TABLE OF CONTENTS

Introduction

[1] Today's students are the first generation to use the Internet for their entire lives! This access to such a global resource offers a myriad of opportunities for learning and personal growth. With this opportunity comes the potential for harm to users of this resource, particularly children and young adults. The Internet Safety Plan, developed by the staff and stakeholders of Danville Public Schools, addresses the need to educate students and adults about the potential dangers of Internet use. It also provides resources for students, teachers, parents, and other stakeholders to enable them to learn how to protect themselves and those in their care.

---

[1] Guidelines and Resources for Internet Safety in Schools, VDOE Division of Technology & Resources, September 2006 V.

Instructional Philosophies and Strategies

Philosophy

The Danville Public School Division will provide educational services of exceptional quality that meet or exceed the needs of each student to achieve exceptional success in life. An essential component of those educational services is provided in the field of technology. The Danville Public Schools ensures equitable access to technology and the use of the Internet to infuse technology into all areas of curriculum and instruction in order to enhance academic achievement. Learners will have the necessary knowledge and skill to interact successfully in a technology-rich environment so they can achieve personal, educational and career goals.

Strategies

- Each District student, or user, will be required to sign an Acceptable Usage Policy (AUP) Agreement. Once this form is on file, a user account will be created and provided to allow access to the Internet and the school network.

- Each teacher or staff member for Danville Public Schools will be given a copy of the Internet Safety Plan (The Plan). This will provide them with a curriculum to follow based on their grade level.

- In addition to a written copy of this document being provided, it will be placed on ERSOLA so that everyone who works for Danville Public Schools will have access.

- Danville Public Schools will have an Internet Safety Week at the beginning of each school year to prepare and inform teachers, students, parents, and the community.

Evaluation and Revision Procedures for Internet Safety Plan (The Plan)

The Internet Safety Plan will be reviewed and revised as needed on an annual basis by instructional and technology staff including members of the Division Technology Committee, Instructional Technology Resource Teacher team, Technical and Program Support Specialists, LAN and WAN analysts and administrative staff. Input from parents and community partners will be solicited as appropriate.

SOLs Covered

CyberSmart's Alignment of Virginia K-8 SOLs and Internet Safety

- C/T K-2.1, C/T K-2.2, C/T K-2.3, C/T K-2.4, C/T K-2.7

- C/T 3-5.3, C/T 3-5.4

- C/T 6-8.3 (a,b) C/T 6-8.4 (a,b) C/T 6-8.5 (a,b)

- C/T 9-12.3 Students will demonstrate knowledge of ethical, cultural, and societal issues related to technology.

- C/T 9-12.4 Students will practice responsible use of technology systems, information, and software.

- C/T 9-12.6 Students will use technology to locate, evaluate, and collect information from a variety of sources.

- C/T 9-12.7 Students will evaluate and select new information resources and technological innovations based on the appropriateness for specific tasks.

Responsibilities

- Employees

  o Classroom Teachers/Long-Term Substitutes/Classified Staff/Media Specialists

  Teachers and staff are responsible for making sure that all students have their assigned log-in and that they are using only their log-in. This also means that teachers will not provide students with access to the teacher log-in. Teachers will assure the District that no one from outside Danville Public Schools is given access to any log-in from the District.

  Teachers will monitor student use of the Internet and Intranet to assure that they are only accessing productive and safe areas. Teachers will prescreen websites prior to providing the link to students. To assist with this, teachers can provide student Internet access with the use of a classroom portaportal. In addition, teachers that do not have portaportal sites can write specific websites on a board, provide them to the students via paper, or have a website added to the student's favorites list. This will diminish the Internet surfing. Also, teachers should remind students that their website visits are not private; any site they visit can be seen and documented in various reports that are viewed by Technology staff.

  To reinforce the idea of Internet safety, teachers are encouraged to place posters around their classrooms/lab that can serve as visual reminders of what you can do to be safe and follow netiquette (*http://www.esafetynorthtyneside.org.uk/article/?id=46559* downloadable posters). Also, topics that are being discussed in the classroom can often be tied to safety/Internet safety. For example, tie in the idea of plagiarism to Copyright and Fair Use when writing a paper using the Internet. Discuss how both ideas are cheating or, in many cases stealing.

  Teachers should also be aware of the current topics or issues that surround the Internet such as: cyberbullying and cyberstalking. Talking to students about these topics periodically reminds students of the dangers that exist on the Internet.

  Any teacher that finds a student using their log-in inappropriately must notify the administration in that building.

  o Instructional Technology Resource Teacher (ITRT)

  ITRTs are responsible for providing classroom teachers and staff a District log-in and providing training on how to properly log in. It is also their responsibility to remind teachers of the proper procedures for Internet and Intranet usage. If an ITRT sees that a teacher or staff member is using their log-in inappropriately, they must report this to the administration of that school.

  In addition, ITRTs will assist teachers in gaining student log-in information and ensuring students know how to log in correctly. ITRTs will also help teachers monitor student usage of the Internet when they are in classrooms.

o Guidance Counselor

Guidance counselors will assist in providing students with information on cyberbullying during classroom, group or individual counseling sessions.

o AUP Holder

The AUP holders are the individuals in the school buildings that are responsible for collecting the signed AUPs from all individuals that will be accessing the Internet/Intranet. This person then requests that a log-in be created for individuals and providing it to the classroom teachers to give to the students. If a signed AUP is not on file, it is the responsibility of the AUP holder to make sure that an account is not provided until a signed AUP is in place.

o Administrators

Administrators in school buildings are responsible for enforcing the AUP that each individual has signed. If a person is found in violation of the AUP, it is the responsibility of the Administrator to enforce consequences. If they find that any adult in the building does not have an account and is entitled to one they should request one to be made by the Human Resources Department. Administrators are responsible for requesting documentation for Internet usage from the WAN Analyst when they feel that a policy has been broken by a student, staff, or member of the faculty.

Administrators must monitor student usage of computers and teacher usage of the Internet within their classrooms. The quality of the websites teachers are using should be reviewed and evaluated for effectiveness.

o School Testing Coordinator (STC)

STCs are responsible for securing testing log-ins for testing purposes only. These log-ins are not to be provided to students directly. They are also responsible for making sure students are not visiting Internet sites that are not directly related to the test being taken.

- Students are required to sign an AUP at the beginning of each school year agreeing to follow DPS guidelines when using the Internet/Intranet. They agree to log in using only their own log-in. They will not visit inappropriate or blocked sites, in any manner. They also agree they will not post or send inappropriate language or images via email or chat rooms. They will follow the Internet Safety curriculum provided by the instructor and will follow online netiquette while doing so. There will be no cyberbullying and any violations for this or any other inappropriate usage of the Internet/Intranet will be reported to the classroom teacher or administrator.

By the time students graduate, they should know:

o how to properly search the Internet;

o proper communication using electronic forms of communication (email, blogs, chat rooms, etc.);

o appropriate and inappropriate information to post on a website (personal data, photos, etc.), why it is appropriate or inappropriate, and how they could be putting themselves at risk;

o how to use netiquette;

4

- o where to go if they feel threatened or violated by something on the Internet;

- o how to protect themselves and their personal information from violators on the Internet.

- Community Stakeholders

  - o Public Library

    While visiting our public libraries, students have the opportunity to use library computers, with various software programs and Internet, which are provided to the public. All individuals that use computers should be made aware of proper Internet usage.

  - o Boys and Girls Club/YMCA/Church-Based Tutorial Programs/Recreational Centers

    Various organizations throughout our community provide computers, software, and Internet access to our students during the day. This allows students to access equipment they may not have at home. With these opportunities also comes the opportunity for the same organizations to educate our students, their parents, and various members of the community on Internet safety, netiquette, and cyberbullying.

  - o Police Department/Social Services

    The police department are aware of the various activities that occur on the Internet. They are available to provide support to schools as well as parents when there is evidence that a student is in danger. They are aware of netiquette and the illegal activities that are occurring in the community via social networks or chat sessions and provide support to end it. Support from the police department is provided in various forms. They can come to schools when an issue has occurred to help resolve it, they are willing to talk to parents in their homes if an incident has occurred, and they are visible as a source of help to the students inside or outside of school.

Safety Measures in Place

- Filtering and Monitoring

  Danville Public Schools provides a web filter that prohibits access to restricted sites. Those restrictions are determined by the software filtering program. Accessibility level for students is much lower than for a teacher. Any site that a student is able to visit that is not being filtered and is deemed an inappropriate site, will be added to the blocked list immediately. All visits to any website by any individual in the District are recorded, monitored and kept indefinitely. A report can be produced at any time to indicate an individual has been trying to access an inappropriate website.

  Data Network Security

  Danville Public Schools has a firewall that stops inbound traffic on unopened ports. Backups are encrypted and it is not accessible to staff.

- Application and Hardware

  o Students

    Each student is given their own unique log-in and password to access their DPS user account. This account provides them access to: their personal documents, the student shared folder, the various pieces of software that have been installed, as well as the Internet.

  o Teachers

    Each teacher is given their own unique log-in and password to access their DPS user account. This account provides them access to: a personal email account, their personal documents, the student folders in their school, the teacher shared folder, the various pieces of software that have been installed, and the Internet.

- Consequences

  At any time, a report detailing both Internet usage and email usage can be created. Inappropriate usage can result in the following actions:

  o Students

    - Loss of Internet access only
    - Loss of network privileges completely
    - Parent conference
    - Suspension

  o Teachers

    - Loss of Internet access only
    - Loss of network privileges completely
    - Reprimand
    - Removal from job responsibilities/loss of job

- Future Implementation

  In the future, a Network Access Control (NAC) will be installed. As technology continues to grow, individuals continue to purchase technology to use within their classrooms. The NAC will allow us to prevent outside hardware from gaining access to Internet while inside school buildings, whether it is an employee within the District or someone in schools from outside the Division.

Integration of Internet Safety into the Classroom

ITRTs throughout the District are responsible for providing the necessary tools to teachers to assist them with integrating Internet Safety into their classrooms.

All teachers or staff members are to be trained in the appropriate method for logging into their District account, and then they are responsible for teaching students the proper method.

Each ITRT is responsible for educating teachers on the proper procedures for using the computers and the Internet, so that they are following the guidelines set by the AUP, and enforcing the rules as the teachers use the computers within the schools. The teachers will then monitor students for the proper procedures and enforce rules supporting proper procedures.

ITRTs and teachers have professional development opportunities, including webinars, to educate everyone on the newest threats to Internet Safety as they are discovered (see Appendix C for professional development website suggestions).

Anyone that finds an individual on a website that is seen as inappropriate is required to notify the WAN administrator of the exact web address so that site can be reviewed and blocked as needed. ITRTs will notify the WAN administrator directly while teachers should notify their school ITRT or building administrator.

There are various things that can be done throughout the District to reinforce the need for safety on the Internet.

- Internet Safety Week: This will be a week set aside each school year to start off the school year in a manner that all individuals in the school district are made aware of Internet Safety and ways they can be safe as their school year progresses. There will be poster contests, guest speakers, parent information sessions, pre-created lesson plans for teachers to use during the week, parental handouts for educating them, and Internet Safety displays throughout the community.   There will be a newsletter that goes home with each student to parents, educating them on Internet Safety.

- All third grade students will be provided with available resources from the Attorney General's Office. This can be used throughout the school year with the classroom teacher as well as with the Media Center.

- As part of the Technology Standard for Instructional Personnel (TSIP), all teachers are required to identify and provide information on Copyright and Fair Use to the ITRT assigned to their building.

- A curriculum is provided for all teachers and for all grade levels through the Internet Safety Plan and on ERSOLA (the Electronic Repository for SOL Activities). This can be used throughout the school year. This curriculum will provide teachers with the objectives, focus, SOLs covered, vocabulary terms, Internet related activities, and extra resources (see Appendix A).

- Within the classrooms and labs, posters can be put up that reinforce the Internet Safety ideas. The posters from the Internet Safety Week contest can be used and changed out as the year progresses (*http://www.esafetynorthtyneside.org.uk/article/?id=46559* downloadable posters).

Community Outreach Activities

The following events/activities could be used to inform the public/community about Internet safety and how it affects the students in the District:

- National Night Out;

- Chalk Talk episodes on Internet Safety;

- Link to DPS website where Internet Safety Plan is located;

- Information to parents about what Internet Safety is in the school newsletters (i.e.; monthly topics);

- PTA Meetings/Parent Education Sessions during the school year;

- Parent workshops (Make-it Take-it Days);

- "Internet Safety Week" throughout the District;

- Classes for students from the guidance departments in the schools;

- Write-ups in ClassCandy (http://classcandy.com/) Newsletter (i.e., monthly topics).

Appendix A: Grade Level Curriculum

Grade Level	Overview	Focus	Objectives	SOLs	Terms	Activities
Kindergarten	Young children need adult guidance when using the Internet.	• Safety	• Students will learn the difference between programs that are on an individual computer and websites. • Students will learn that when visiting websites, they need to think safety first.	• C/T K-2.1 • C/T K-2.2 • C/T K-2.3 • C/T K-2.4 • C/T K-2.7	• Internet (the Web) • Websites	• Go Places Safely • Kids Rules for Online Safety • D.A.R.E. Activity Lessons • CyberSmart K and 1st Grade Lesson Ideas • Net Smartz Games • Infinite Learning Lab
1st	Children need to learn to use the computer and the Internet in a safe, honest, and respectful manner.	• Computer ethics	• Students will learn that material found on the computer is someone's property and needs to be respected. • Students will learn how to cite material found on the computer through teacher modeling.	• C/T K-2.1 • C/T K-2.2 • C/T K-2.3 • C/T K-2.4	• Internet • Copyright	• Kids Rules for Online Safety • iKeepSafe.org • NetSmartz Video and Games • Online Safety Video • Internet Safety Video • NetSmartz Video and Games • Infinite Learning Lab

Grade Level	Overview	Focus	Objectives	SOLs	Terms	Activities
2nd	Children need to recognize the need for privacy and how to protect their privacy.	• Protecting personal information	• Students will understand the difference between web page content and advertising on the page, as well as pop-up window advertisements. • Students will understand the importance of protecting personal information and passwords.	• C/T K-2.3 • C/T K-2.4 • C/T K-2.5 • C/T K-2.6 • C/T K-2.7	• Webpage • Advertising • Password • Pop-up Windows	• What's Private • Netsmartz • Safety Land • The Webville Outlaws • Clicky's Challenge • The Password Rap • First Adventures of the Three Cyberpigs • Internet Safety and You • Internet Safety Game • Cyberethics for Kids • Safe Surfing with Doug • Kids in the Know • McGruff • Webonauts Internet Academy • Safety Tips and Advice • Surfing Scavenger Hunt • CyberSmart's 2nd/3rd Grade Lesson Ideas • Kids Rules for Online Safety • Yahoo! Internet Safety Tips • Disney Internet Safety • Infinite Learning Lab • Get Cybersmart with Phineas and Ferb • 3 Little Cyber Pigs Game #1 • 3 Little Cyber Pigs Game #2 • Cyber Treehouse

Grade Level	Overview	Focus	Objectives	SOLs	Terms	Activities
3rd	Children need to recognize the need for privacy and how to protect their passwords.	• Student Privacy • Strong Passwords	• Students will understand the importance of keeping personal information private. • Students will understand and create strong passwords.	• C/T 3-5.3 • C/T 3-5.4	• Identity theft • Instant messaging • Phishing • Spam • Chat rooms • Online	• Meet the WizzyWigs • The Carnegie Cyber Academy • What's Private • Netsmartz • Safety Land • The Webville Outlaws • Clicky's Challenge • The Password Rap • First Adventures of the Three Cyberpigs • Internet Safety and You • Kids in the Know • McGruff • Webonauts Internet Academy • Safety Tips and Advice • Surfing Scavenger Hunt • CyberSmart's 2nd/3rd Grade Lesson Ideas • Kids Rules for Online Safety • Yahoo! Internet Safety Tips • Disney Internet Safety • Infinite Learning Lab • Safe Surfing Quiz • Get Cybersmart with Phineas and Ferb • 3 Little Cyber Pigs Game #1 • 3 Little Cyber Pigs Game #2 • Cyber Treehouse

Grade Level	Overview	Focus	Objectives	SOLs	Terms	Activities
4th	Children need to learn that not all people are who they say they are on the Internet.	• Never meet people in real life that you met online. • Things you do on the Internet leave an Internet footprint.	• Students will understand that strangers from the Internet may not always be who they say they are. • Students will understand that they should never meet people in real life that they meet online. • Students will explore how information put on the Internet can be seen by others, and stay there forever.	• C/T 3-5.3 • C/T 3-5.4	• Identity theft • Instant messaging • Phishing • Spam • Chat room • Cyberbully • Internet footprint	• Privacy Rules • Lesson Plan on Safe Talking • Lesson Plan on Being a Good Internet Citizen • Lesson Plan on Email and IM • Kids Rules for Online Safety • Who's Your Friend on the Internet • Resources for Parents • iKeep Safe Coalition • Alternative Game Infinite Learning Lab • Safe Surfing Quiz • Get Cybersmart with Phineas and Ferb • 3 Little Cyber Pigs Game #1 • 3 Little Cyber Pigs Game #2 • Cyber Treehouse

Grade Level	Overview	Focus	Objectives	SOLs	Terms	Activities
5th	Children need to recognize that there are bad people that prey on children on the Internet and the need to tell an adult if they feel uncomfortable with anything they do on the Internet.	• Privacy • Networking • Dangers on the Internet • Self-filtering	• Students will evaluate whether Internet content is appropriate or inappropriate material. • Students will understand the importance of telling an adult, so that other younger children will not be exposed. • Students will understand basic concept of "being watched" on the Internet and making decisions based on privacy. • Students will understand that there are bad people who may use the Internet to prey on children. • Students will demonstrate knowledge of information protection and strong passwords.	• C/T 3-5.4	• Identity theft • Instant messaging • Phishing • Spam • Chat rooms	• The Boy Who Loved IM, and Lesson Plans • Kids Rules for Online Safety • Tracking Teresa • "Rating Web Sites" • iKeep Safe Coalition • Alternative Game • PBS Kid's License • KidsCom Internet Safety Game • Pledge Sheet • Infinite Learning Lab • Safe Surfing Quiz • Get Cybersmart with Phineas and Ferb • 3 Little Cyber Pigs Game #1 • 3 Little Cyber Pigs Game #2 • Cyber Treehouse

Grade Level	Overview	Focus	Objectives	SOLs	Terms	Activities
6th	Students need to recognize what constitutes cyberbullying and ethical issues relating to technology and the Internet.	• Cyberbullying • Copyright	• Students will demonstrate knowledge of ethical, cultural and societal issues related to technology (password privacy, creating strong passwords, sharing information online). • Students will demonstrate responsible use of information and software, including abiding by copyright regulations and the Division's AUP. • Students will describe what constitutes cyberbullying and understand the ramifications.	• C/T 6-8.3 (a,b) • C/T 6-8.4 (a,b) • C/T 6-8.5 (a,b)	• Cyberbullying • Cybercrime • Cyber Security • Predators • Copyright and Fair Use	• Stop Cyberbullying • Brain Pop Cyberbullying • Cyber Smart Cyberbullying Lesson Plan • Dealing with Cyberbullying • Cyberbullying: Feathers On the Wind • Cyberbullying: Broken Friendship 1 • Cyberbullying: You Can't Take It Back • iSafe Cyberbullying • No More Bullying: Understanding the Problem • Building Bully-free Environments • CyberSmart Lessons and Discussion Ideas • NetSmartz Online Resources Page • Forensic Problem Solving: The Vanishing Videos Mystery • Don't Be Fooled by a Photograph • Internet Safety Statistics • Citation Machine • Copyright Quiz • Cyber Bee • Visit Copyright Bay • Is it Copyright Infringement? • Copyright Issues • McGruff's Internet Safety Pledge • Safe Families Internet Safety Pledge • Protect Kids Internet Safety Pledge • Go Girls Only Internet Safety Pledge • Parent/Student Internet Safety Pledge • PC Tattletale's Internet Safety Pledge • Get Cybersmart with Phineas and Ferb • 3 Little Cyber Pigs Game #1 • 3 Little Cyber Pigs Game #2 • Cyber Treehouse • My Space Quiz

Grade Level	Overview	Focus	Objectives	SOLs	Terms	Activities
7th	Students need to learn how to evaluate Web content for accuracy and steps to protecting their identity.	• Evaluation of websites • Protecting your identity • Instant messaging and online chatting	• Students will demonstrate knowledge of email safety, viruses, chat rooms, and predators. • Students will learn how to evaluate websites for accuracy and bias. • Students will understand steps to take to protect their identity.	• C/T 6-8.3 (a,b) • C/T 6-8.4 (a,b) • C/T 6-8.5 (a,b)	• Blogging • Chat rooms • Cyber stalking • File sharing • Filter • Instant messaging • Phishing • Social networking • Viruses • Spyware	• Stop Cyberbullying • Brain Pop Cyberbullying • Cyber Smart Cyberbullying Lesson Plan • Dealing with Cyberbullying • Cyberbullying: Feathers On the Wind • Cyberbullying: Broken Friendship 1 • Cyberbullying: You Can't Take It Back • iSafe Cyberbullying • No More Bullying: Understanding the Problem • Building Bully-free Environments • Good Messaging Manners • Tracking Teresa • Chat Danger • ID the Creep • Julie's Journey • Amy's Choice • Identifying High Quality Sites • CyberSmart Lessons and Discussion Ideas • NetSmartz Online Resources Page • Real Life Stories • Evaluating Web Pages for a Class Collection • Citation Machine • Copyright Quiz • Cyber Bee • Visit Copyright Bay • Is it Copyright Infringement? • Copyright Issues • NetSmartz Internet Safety Pledge for Middle • McGruff's Internet Safety Pledge • Safe Families Internet Safety Pledge • Protect Kids Internet Safety Pledge • Go Girls Only Internet Safety Pledge • Parent/Student Internet Safety Pledge • PC Tattletale's Internet Safety Pledge • Power and Responsibility Lesson Plan • Online Etiquette Quiz • Core Rules of Netiquette • Netiquette for Kids • Internet Etiquette • Netiquette Quiz • Get Cybersmart with Phineas and Ferb • My Space Quiz

Grade Level	Overview	Focus	Objectives	SOLs	Terms	Activities
8th	Students need to be aware of the dangers of online predators.	• Plagiarism • Social Networking • Predators	• Students will discuss appropriate use of technology and the need for laws governing its use. • Students will understand the dangers associated with the following: blogging, chat rooms, email, file sharing. • Students will demonstrate responsible use of an email account. • Students will learn about the dangers associated with social networking and the need to keep all personal information private.	• C/T 6-8.3 (a,b) • C/T 6-8.4 (a,b) • C/T 6-8.5 (a,b)	• Identity theft • Spam • Internet footprints • Web 2.0 • Blog • Wiki	• Savvy Online Talk and Messaging • Privacy, What's the Big Deal • Good Messaging Manners • Check the Privacy Policy • Can You Hack It • Social Networking - Post-to-be-Private • Internet Safety Pledge for Middle and High School • Real Life Stories • Online Resources Page • Get Net Wise • ID Creep • Copyright and Fair Use • Infinite Learning Lab • Internet Safety Plan Lesson Plan • Connect Safely • Wired Safely • Child Net International • Get Cybersmart with Phineas and Ferb • Digital Citizenship • Cell Phone Tips • Instant Messaging Help • Safety Using YouTube • Chat Danger • My Space Quiz

Grade Level	Overview	Focus	Objectives	SOLs	Terms	Activities
9th through 12th	Integrating Internet Safety and Digital Ethics into the high school classroom	• Cyber Character: Social Networking • Cyber Security • Personal Safety: Online Communications, Email, IM, Chat Rooms, Blogs, and Gaming • Personal Safety: Cyber Predators	• Students will demonstrate knowledge of ethical, cultural, and societal issues related to technology. • Students will practice responsible use of technology systems, information, and software. • Students will use technology to locate, evaluate, and collect information from a variety of sources. • Students will evaluate and select new information resources and technological innovations based on the appropriateness for specific tasks.	• C/T 9-12.3 • C/T 9-12.4 • C/T 9-12.6 • C/T 9-12.7	• Cyberbully • Disclosure • Privacy • Social networking • Privacy setting • Stalker • DOPA • AUP • Urban Legend • Hoax • Secure password • Harassment • Griefer • Dissing • Cyber harassment • Identity theft • Malicious code • Phishing • Pharming • Spyware • Fraud	• [CyberSmart Lessons and Discussion Ideas for Grades 9 - 12](#) • [Plagiarism Flash Activity #1](#) • [Plagiarism Activity #2](#) • [Plagiarism Activity #3](#) • [Privacy...Google Expose'](#) • [ID The Creep](#) • [NetSmartz Online Resources Page](#) • [Webquest on Internet Safety](#) • [Think Before you Post](#) • [Making Good Decisions](#) • [Your Online Image](#) • [Cyberbulling: Broken Friendships](#) • [Managing Passwords](#) • [Dangers in MySpace](#) • [Online Identity Theft Activity](#) • [Managing Passwords](#) • [Connected 24/7](#) • [Acceptable Social Networking?](#) • [(Cyberbullying: You Can't Take It Back)](#) • [WebWiseKids.org](#) • [My Space Quiz](#) • [Sorted](#)

Appendix B: Glossary and Websites to use as Resources for Terms
(http://www.doe.virginia.gov/support/safety_crisis_management/Internet_safety/guidelines_resources.pdf)

Blog/Blogging: This term is derived from *Web log* and is an increasingly popular type of website. Most take the form of journal entries and allow readers to post comments.

Net Family News:
http://www.google.com/custom?domains=www.netfamilynews.org&q=blogging&sitesearch=www.netfamilynews.org&client=pub-1326885308549211&forid=1&ie=ISO-8859-1&oe=ISO-8859-1&safe=active&cof=GALT%3A%23009999%3BGL%3A1%3BDIV%3A%23333333%3BVLC%3A000000%3BAH%3Acenter%3BBGC%3AFFFFFF%3BLBGC%3AFFFFFF%3BALC%3A009999%3BLC%3A009999%3BT%3A000000%3BGFNT%3ACC0000%3BGIMP%3ACC0000%3BLH%3A50%3BLW%3A108%3BL%3Ahttp%3A%2F%2Fwww.netfamilynews.org%2FNFNlogoGoogle.gif%3BS%3Ahttp%3A%2F%2Fwww.netfamilynews.org%3BFORID%3A1%3B&hl=en

NetsSmartz Bulletin by National Center for Missing & Exploited Children and Boys & Girls Clubs of America: http://www.netsmartz.org/Blogging

Blogsafety by Childnet International: http://www.childnet-int.org/blogsafety/

Bookmark(s): This browser feature stores a Web address in memory and allows the user to link quickly to the site.

TechTerms.com: http://www.techterms.com/definition/bookmark

TechnologyDictionary.com by Art Branch Inc.: http://www.techdict.org/define/bookmark/

Chat Rooms: These websites or online services facilitate electronic discussions by quickly posting the comments and responses of multiple users.

EHow.com by Demand Media: http://www.ehow.com/facts_5132939_definition-chat-room.html

GetNetWise: Chat by Internet Education Foundation:
http://kids.getnetwise.org/safetyguide/technology/chat

Computer Monitoring: The technique of tracking Internet sites by looking at the *history* of the browser. It also refers to software used for the same purpose.

EHow.com by Demand Media:
http://www.ehow.com/facts_6896970_computer-monitoring-definition.html

YourDictionary.com by LoveToKnow: http://computer.yourdictionary.com/computer-monitoring

Cyberbullies/Cyberbullying: Online threats by one student toward another, typically through emails or on websites (e.g., *blogs, social networking* sites).

Be Web Aware: Challenging Cyberbullying by Media Awareness Network:
http://www.bewebaware.ca/english/CyberBullying.aspx

Cyberbully.org: http://www.cyberbully.org/

TechTerms.com: http://www.techterms.com/definition/cyberbullying

Cyberbullying: *Research* by Cyberbully.us: http://www.cyberbullying.us/research.php

Real-Life Stories by NetSmartz: http://www.netsmartz.org/resources/reallife.htm

STOP Cyberbullying by WiredKids: http://www.stopcyberbullying.org/index2.html

Resource for youth that have been targets of bullies: www.cyberbully411.org

Cybercrime: Any Internet-related illegal activity.

TechTerms.com: http://www.techterms.com/definition/cybercrime

Cybersecurity (sometimes *cyber security*): Any technique, software, etc., used to protect computers and prevent online crime.

US-CERT U.S. Computer Emergency Readiness Team home page: http://www.uscert.gov/

YourDictionary.com by Love to Know: http://computer.yourdictionary.com/cybersecurity

Cyberstalking: Methods individuals use to track, lure, or harass another person online.

Cyberguard from the U.S. Department of Justice: http://www.cyberguards.com/CyberStalking.html

YourDictionary.com by LoveToKnow: http://law.yourdictionary.com/cyberstalking

MacMillianDictionary.com: http://www.macmillandictionary.com/dictionary/british/cyberstalking

Digital Footprints: Computers maintain a record of all website visits and email messages, leaving a trail of the user's activity in cyberspace. This data can still exist even after the browser *history* has been cleared and email messages have been deleted.

Digital Legacy by Creative Commons Attribution:
http://*learningischange*.com/2009/05/20/digital-legacy-lesson-plans/#

Email: A system for sending messages from one individual to another via telecommunication links between computers.

GetNetWise: *Risks* by Technology: Email by Internet Education Foundation:
http://kids.getnetwise.org/safetyguide/technology/email

OnGuard Online: Spam Scams by Federal Trade Commission: http://onguardonline.gov/spam.html

Sorted.com by Childnet International: http://www.childnet-int.org/sorted/

Favorite(s): The name for *bookmarks* (see above) used by Microsoft's Internet Explorer browser.

TechTerms.com: http://www.techterms.com/definition/favorites

About.com: http://browsers.about.com/od/webbrowserglossary/g/favorites.htm

YourDictionary.com by Love to Know Corp: http://computer.yourdictionary.com/favorites

File Sharing: Software that enables multiple users to access the same computer file simultaneously. File sharing sometimes is used illegally to download music or software.

OnGuard Online: P2P File-Sharing by Federal Trade Commission: http://onguardonline.gov/p2p.html

Sorted.com by Childnet International: http://www.childnet-int.org/sorted/trojansviruses.aspx

Filter/Filtering: Software that screens and blocks online content.

Filtering and Blocking by WiredKids: http://www.wiredkids.org/safesites/filtering.html

Your dictionary.com by Love to Know: http://computer.yourdictionary.com/filter

Gaming: Internet games which can be played either individually or by multiple online users at the same time.

Griefers: Internet users who intentionally cause problems for other *gamers.*

WorldIQ.com: http://www.wordiq.com/definition/Griefing

FreeDictionary.com by Farlex: http://encyclopedia.thefreedictionary.com/griefer

Grooming: Techniques sexual predators use to get to know their victims in preparation for sexual abuse.

Predator Tip Sheet by i-SAFE: http://xblock.isafe.org/docs/Eluding_Internet_Predators_Tip_Sheet.pdf

Hate Sites: Websites that promote hatred.

Protecting Children and Teens from Online Hate by Media Awareness Network: http://www.media-awareness.ca/english/issues/online_hate/protect_child_hate.cfm

History: A tracking feature of Internet browsers that shows all the recent websites visited.

TechnologyDictionary.com by Art Branch Inc.: http://www.techdict.org/define/bookmark/

YourDictionary.com by LoveToKnow: http://computer.yourdictionary.com/history

WebDeveloperNotes.com: http://www.webdevelopersnotes.com/basics/what-is-browser-history.php

Identity Theft: A crime in which someone obtains vital information (e.g., credit card, Social Security, bank account numbers) of another person, usually to steal money. Email scams, *spyware*, and *viruses* are among the most typical methods for stealing someone's identity.

OnGuard Online: ID Theft by Federal Trade Commission: http://onguardonline.gov/idtheft.html

About.com: http://idtheft.about.com/od/glossary/g/Define_IDTheft.htm

Dictionary.com: http://dictionary.reference.com/browse/identity+theft

SecuritySearch.com by Tech Target: http://searchsecurity.techtarget.com/sDefinition/0,sid14_gci801871,00.html

Instant Message/Messaging: Known by the acronym *IM*, this is a variation of *chat rooms* that allows users to communicate through text messages.

Dictionary.com: http://dictionary.reference.com/browse/instant+messaging

YourDictionary.com by Love to Know: http://computer.yourdictionary.com/instant-messaging

Malicious Code: A computer code that is intentionally introduced into a system to damage or destroy files or disrupt the operation of a computer.

YourDictionary.com by Love to Know: http://computer.yourdictionary.com/malicious-code

Aladdin.com by Aladdin Knowledge Systems: http://www.esafe.com/csrt/malicious-code.aspx

The Geneva Police Department, Geneva, IL.: http://www.geneva.il.us/pd/PDFFiles/MaliciousCode.pdf

Peer-to-peer (P2P) Computing: A popular way for Internet users to share one another's computer files - usually music, game, or software files.

OnGuard Online: P2P File-Sharing by Federal Trade Commission: http://onguardonline.gov/p2p.html

Sorted.com by ChildNet International: http://www.childnet-int.org/sorted/filesharing.aspx

Phishing: This scam involves sending a fraudulent email soliciting credit card, Social Security, or other personal information from an unsuspecting user.

TechTerm.com: http://www.techterms.com/definition/phishing

How Stuff Works by The Discovery Channel: http://computer.howstuffworks.com/phishing.htm

Sorted.com by Childnet International: http://www.childnet-int.org/sorted/spamphishing.aspx

Proxy Sites: These parallel websites allow children to get around some *filtering* software and access sites that have been blocked.

Social Networking: Online communities where people share information about themselves, music files, photos, etc. There are many social networking websites (e.g., MySpace, Facebook, or Friendster).

ChatDanger: How to Keep SAFE While Chatting Online by Childnet International:
http://www.chatdanger.com/

ConnectSafely Forum by Tech Parenting Group: http://www.blogsafety.com/

GetNetWise: Social Networking Sites by Internet Education Foundation:
http://kids.getnetwise.org/safetyguide/technology/socialnetworking

Social Networking Sites: Safety Tips for Tweens and Teens by Federal Trade Commission:
http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.pdf

Spam: Unsolicited email or junk mail. Most spam is either a money scam or sexual in nature. Internet Service Providers, email software, and other software can help block some, but not all, spam.

TechTerms.com: http://www.techterms.com/definition/spam

Sorted.com by Childnet International: http://www.childnet-int.org/sorted/spamphishing.aspx

How Stuff Works by Discovery Education:
http://*computer*.howstuffworks.com/Internet/basics/spam.htm

TechnologyDictionary.com: http://www.techdict.org/define/spam/

Spyware/Adware: Software installed on user's computers without their knowledge. The programs typically will track computer use and create numerous pop-up ads. In some instances, the spyware can damage the computer and facilitate *identity theft*.

TechTerms.com: http://www.techterms.com/definition/spyware

Sorted.com by Childnet International: http://www.childnet-int.org/sorted/spywareadware.aspx

How Stuff Works by Discovery Education: http://computer.howstuffworks.com/spyware.htm

Technology Dictionary.com: http://www.techdict.org/define/spyware/

Viruses: Software programs that typically arrive through email attachments and multiply on the hard drive, quickly exhausting the computer's memory. A *trojan* is a variation that allows unauthorized users access to the computer, from which they can send infected emails or *spam*.

TechTerms.com: http://www.techterms.com/definition/virus

Sorted.com by Childnet International: http://www.childnet-int.org/sorted/trojansviruses.aspx

TechnologyDictionary.com: http://www.techdict.org/define/virus/

Wireless Computers: Many networks now allow computers access to the Internet without being connected with wires. These networks are becoming increasingly more popular and powerful, allowing people to access the Internet using cell phones and other devices.

GetNetWise: Spotlight on Wireless Security by GetNetWise: http://spotlight.getnetwise.org/wireless/

WEBSITES FOR HELP WITH TERMS AND DEFINITIONS

Glossary by Symantec: http://securityresponse.symantec.com/avcenter/refa.html

Internet Definitions by Netsmartz: http://www.netsmartz.org/safety/definitions.htm

The Librarian's Guide to Great Web Sites for Kids by American Library Association:
http://www.ala.org/ala/aboutala/offices/oif/iftoolkits/litoolkit/2003internettoolkit.pdf

OnGuard Online: Glossary by Federal Trade Commission: http://onguardonline.gov/glossary.html

Appendix C: Web-Based Resources
(http://www.doe.virginia.gov/support/safety_crisis_management/Internet_safety/guidelines_resources.pdf)

I. Teacher Resources

Age-Appropriate Guidelines for Internet Use

Be Web Aware by Media Awareness Network: http://www.bewebaware.ca/english/default.aspx

GetNetWise: Online Safety Guide by Internet Education Foundation:
http://kids.getnetwise.org/safetyguide/

Ethics

Cyberethics by U.S. Department of Justice, Computer Crime & Intellectual Property Section:
http://www.cybercrime.gov/cyberethics.htm

How the Internet Works

How Does the Internet Work? by U&I Learning (commercial site - no advertising):
http://hwi.uni.be/archief/en/index.htm

How Internet Infrastructure Works by Jeff Tyson for HowStuffWorks:
http://computer.howstuffworks.com/Internet-infrastructure.htm

The Internet Tutorial by Dynamic Web Solutions (commercial site - no advertising):
http://www.dynamicwebs.com.au/tutorials/history.htm

International, National, and State Organizations

ChildNet International home page: http://www.childnet-int.org

GetNetWise home page by Internet Education Foundation: http://www.getnetwise.com/

Internet Safety by Polly Klaas Foundation: http://www.pollyklaas.org/Internet-safety/index.html

i-SAFE home page by Internet Safety Foundation: http://www.isafe.org/

National Center for Missing & Exploited Kids home page: http://www.missingkids.com/

NetSmartz Workshop by National Center for Missing & Exploited Kids:
http://www.netsmartz.org/http://www.netsmartz.org/espanol/ (Spanish)

OnGuard Online home page by Federal Trade Commission: http://onguardonline.gov/index.html

ProtectKids.com home page by Enough Is Enough: http://www.protectkids.com/

SafeKids.com home page: http://www.safekids.com/

Safe Surfin' Foundation home page: http://www.safesurfincentral.org/

Virginia Center for School Safety home page by Virginia Department of Criminal Justice Services: http://www.dcjs.virginia.gov/vcss/?menuLevel=5

WiredSafety.org home page by WiredKids (includes *Teenangels*, *WiredSafety*, and *WiredKids*): http://www.wiredsafety.org/

Internet Benefits and Risks

Cybercrime by National Association of Attorneys General: http://naag.org/publications_cybercrime.php

GetNetWise: What are the Risks for Children Online? by Internet Education Foundation: http://kids.getnetwise.org/safetyguide/danger/

Parenting Online by WiredKids: http://wiredkids.org/parents/parentingonline/index.html
http://wiredkids.org/resources/documents/pdf/parentingonline.pdf (Printable version)
http://*www*.wiredkids.org/parents/parentingonline/parentingonline-ES-v1.pdf (Spanish version)

The Positives and Perils of the Internet: Working Together to Make Your Family's Online Experience Safe and Fun by Donna Rice Hughes for ProtectKids.com: http://www.protectkids.com/parentsafety/positive_peril.htm

Lesson Plans/Curricula

Activities and Lessons by Wired Safety: http://www.wiredsafety.org/wiredlearning/toc.html

Cyberethics for Teachers: A Lesson Plan Outline for Elementary and Middle School Children by U.S. Department of Justice: http://www.cybercrime.gov/rules/lessonplan1.htm

Digital Ethics by Nortel LearniT: http://www.nortellearnit.org/LearniT/technology/Digital_Ethics/

Educational Games by Media Awareness Network: http://*www*.media-awareness.ca/english/games/index.cfm

Online Safety by Nortel LearniT: http://www.nortellearnit.org/LearniT/technology/Online_Safety/

Safe Passage: Introduction by Media Awareness Network: http://www.media-awareness.ca/english/teachers/wa_teachers/safe_passage_teachers/index.cfm

Professional Development

Information Literacy and the Net: http://bellinghamschools.org/sites/default/files/studentgal/onlineresearch/oldonline/literacy.htm

Every K-12 Professional's Guide to the New Literacies Associated with Information and Communication Technology (ICT) and Higher Student Achievement by CyberSmart!: http://www.cybersmart.org/pd/ or http://www.cybersmart.org/info/overview_pres.asp

i-LEARN home page by i-SAFE: http://ilearn.isafe.org/

Reporting Problems

CyberTipline by National Center for Missing & Exploited Children: http://www.cybertipline.com/

GetNetWise: Reporting Trouble by Internet Education Foundation:
http://kids.getnetwise.org/trouble/

Internet Crime Complaint Center home page by FBI and National White Collar Crime Center:
http://www.ic3.gov/

OnGuard Online: File a Complaint by Federal Trade Commission:
http://onguardonline.gov/filecomplaint.html

Report a CyberCrime by ProtectKids.com: http://www.protectkids.com/report/index.htm

Sites for Educators

Computer Security Resource Center by National Institute of Standards and Technology, Computer Security Division: http://csrc.nist.gov/

Cyberethics for Teachers: A Lesson Plan Outline for Elementary and Middle School Children by U.S. Department of Justice: http://www.cybercrime.gov/rules/lessonplan1.htm

EDUCAUSE CONNECT browse page: http://www.educause.edu/Browse/645?PARENT_ID=702

Media Literacy-National Perspective by the State Education Technology Directors Association (SETDA): http://www.setda.org/web/guest/toolkit2007/medialiteracy/nationalperspective

Play It Cyber Safe: Resources by Business Software Alliance:
http://www.playitcybersafe.com/resources/index.cfm

Safe and Responsible Use of the Internet: A Guide for Educators by Center for Safe and Responsible Internet Use: http://csriu.org/onlinedocs/pdf/srui/sruilisting.html

Safe and Secure? by Scholastic: http://content.scholastic.com/browse/article.jsp?id=127

Safeguarding Your Technology by U.S. Department of Education, National Center for Education Statistics: http://nces.ed.gov/pubs98/safetech/

7 Things You Should Know About by EDUCAUSE:
http://www.educause.edu/7ThingsYouShouldKnowAboutSeries/7495

Virginia Alliance for Secure Computing and Networking home page: http://vascan.org/

WiredKids: Educators by WiredKids: http://www.wiredkids.org/educators/index.html

II. **Parent Resources**

Parent/Child Sample Agreements

Family Contract for Online Safety by SafeKids.com: http://www.safekids.com/contract.htm

Rules 'N Tools Youth Pledge by ProtectKids.com:
http://www.protectkids.com/parentsafety/pledge.htm

Reporting Problems

CyberTipline by National Center for Missing & Exploited Children: http://www.cybertipline.com/

GetNetWise: Reporting Trouble by Internet Education Foundation:
http://kids.getnetwise.org/trouble/

Internet Crime Complaint Center home page by FBI and National White Collar Crime Center:
http://www.ic3.gov/

OnGuard Online: File a Complaint by Federal Trade Commission:
http://onguardonline.gov/filecomplaint.html

Report a CyberCrime by ProtectKids.com: http://www.protectkids.com/report/index.htm

Sites for Parents

News *service* for parents to keep up with the most recent events in technology news:
www.netfamilynews.org

Common Sense Internet Safety Guide by Common Sense Media:
http://www.commonsense.com/download/index.php

Don't Believe the Type: For Parents and Guardians by NetSmartz:
http://tcs.cybertipline.com/parentsguardians.htm

GetNetWise: Safety Tips for Families by Internet Education Foundation:
http://kids.getnetwise.org/safetyguide/families

Internet Survival Guide for Parents by Commonsense Media:
http://www.commonsense.com/Internet-safety-guide/

i-LEARN Online by i-SAFE: http://ilearn.isafe.org/

Keeping Children Safe Online by U.S. Computer Emergency Response Team:
http://www.us-cert.gov/cas/tips/ST05-002.html

Parents by *National* Crime Prevention Council: http://www.ncpc.org/topics/by-audience/parents

A Parent's Guide to Internet Safety by FBI: http://www.fbi.gov/publications/pguide/pguidee.htm

A Parent's Guide to Online Kids by The Children's Partnership:
http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches_and_Presentations&CONTENTID=9071&TEMPLATE=/CM/ContentDisplay.cfm

The Parent's Guide to the Information Superhighway: Rules and Tools for Families Online by The Children's Partnership:
http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches_and_Presentations&CONTENTID=4687&TEMPLATE=/CM/HTMLDisplay.cfm

Parent's Rules 'N Tools by ProtectKids.com: http://www.protectkids.com/parentsafety/index.htm

Safe Surfin' Foundation home page by safesurfincentral.org: http://www.safesurfincentral.org/

Social Networking Sites: A Parent's Guide by Federal Trade Commission:
http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.pdf

10 Common Questions about Internet Safety by iKeepSafe.org and Symantec:
http://www.ikeepsafe.org/iksc_partners/symantec/

What Parents Can Do About Internet Safety by Larry Magid for Safekids.com:
http://www.safekids.com/articles/parents_can.htm

WiredKids: Parents by WiredKids: http://www.wiredkids.org/parents/index.html