Jennie Dean Elementary School

Technology Plan 2011-2016

Jennie Dean Elementary School

9601 Prince William ST
Manassas, Virginia 20110
(571) 377-6300

Dr. Robin Toogood
Principal

Athraa Dawhi

Instructional Technology Training Specialist

Computer Teacher Katrina Ward

Technology Committee

Amanda Griffith

Christina Thai Papa

Lauren Tierney

Table of Contents

Dean Elementary School Overview

Dean Elementary School is located at 9601 Prince William Street in Manassas, Virginia. It is an example of educational change and growth for over 100 years. Our founder was Jennie S. Dean, the daughter of Charles and Annie Dean, born in Sudley Springs, Virginia. The legacy began in 1893 when Jennie Dean had a dream to build an industrial or vocational school where Black children could learn a useful trade. In spite of numerous attempts and tragedies, the Manassas Industrial School continued to thrive and matured to serve approximately 500 students. Boys learned valuable trades such as agriculture, carpentry, masonry, electricity, plumbing and welding. Girls became proficient in cooking, sewing and gardening. The school survived throughout Jennie Dean's life. Jennie Dean remained involved in the various aspects of the school until her death on May 3, 1913. The school continued to educate its young black students after her death. In 1938 Prince William, Fairfax, and Fauquier Counties agreed to purchase the institution and operated it as a regional high school for Blacks. The City of Manassas established its own public school system in 1977. Jennie Dean became a middle school. Thirteen years later, Jennie Dean was renovated and reopened as an elementary school. Our school campus is unique with its historical site.

Our school is home to preschool through fourth grades, to include special education and ESOL programs. Our curriculum is aligned with the Standards of Learning as set forth by the Virginia Department of Education and the City of Manassas Public Schools Program of Studies. The legacy of Jennie Dean continues with a rich heritage.

Department of Instructional Technology and Administrative Technology

The Instructional Technology Training Specialist and Network Administrator work in support toward ensuring the success of the Manassas City Public Schools Technology Initiative. The instructional technology staff consists of one Instructional Technology Training Specialist (ITTS) and one Network Administrator.

Athraa Dawhi	Instructional Technology Specialist
Brian Florack	Network Administrator

In addition, there exists the Dean Technology Committee whose purpose is to address school technology issues and support each school's technology program through research, training, innovation, and collaboration. The Dean Technology Advisory Committee consists of

one Instructional Technology Specialist, six teachers, one Network Administrator, two specialists, two Instructional Assistants, and the building principal. The committee is open to all staff and administrators.

The main focus of the instructional technology staff is to foster 100% technology integration in all curriculum areas. One goal of the instructional technology staff is to continue to work with all instructional staff in introducing technologies that would provide real-time assessment opportunities for students and teachers. Our efforts will continue with further implementation of and training in the usage of SchoolNet , iPads, Smartboards, Smart response, Elmo camera and the VLE which is Manassas City Public School's e-learning system or Virtual Learning Environment (VLE).

Another goal is to increase the exposure of the Dean instructional staff to the latest emerging technologies currently in the K-12 environment. This will include continuation of the expansion of multimedia and wireless technologies division-wide, which will take into consideration handheld technologies, interactive whiteboards, and wireless laptops. An additional example of an emerging technology is the integration of video streaming technologies into the K-12 environment. United Streaming will continue to be used by Dean instructional staff for this purpose. Finally, the establishment of online instructional opportunities is imperative in order to support the enhancement of classroom integration practices.

The Administrative Technology Department provides a level of technical support and maintenance for approximately 200 computers/laptops, 55 printers, 1 network server and all peripheral equipment to ensure that we are promoting efficiency in the administrative and instructional areas. The Local Area Network (LAN) at Dean provides high speed network access to all areas with backbone speeds connecting network closets at 1GBs and connections to

desktop computers are 100MBs. Wireless Access Points running at 54MBs are installed throughout the school system to provide a secure wireless network for laptops, PDA's etc... The job of the network administrator is to maintain and support the LAN network and other equipment at Dean.

Executive Summary

Dean Elementary School, in order to prepare students for the 21st century, is committed to providing access to and education in the use of emerging technologies. Essential skills for the 21st century include communication, publication, knowledge building, research, problem solving, experimentation, and construction. The ability to be able to acquire, evaluate, utilize vast amounts of information, and the No Child Left Behind Act of 2001, reinforces the importance of continued support for technology to provide, extend, and enrich learning opportunities for all stakeholders.

Dean Elementary School is dedicated to ensuring that technology is integrated into all aspects of the curriculum, instruction, assessment, and every day school management. It is our intention that technology will play a fundamental role in providing, extending and enriching learning opportunities for all students and the learning community. To accomplish this endeavor, Dean Elementary School is also emphasizing increased professional development opportunities for its staff and administration.

This plan is designed to serve as framework for the utilization of technology within Dean and to inform decision makers as to the allocation and need for continued resources for technology. Additional input will be solicited from students and community members. Distribution of the technology plan will be conducted via the Dean website. A copy will also be placed in the Dean library so that all stakeholders are aware of the goals and strategies.

Five goals have been developed for the Dean technology plan and are aligned with the components of the MCPS Technology Plan and the components required by the Virginia Department of Education.

The five goals of the new state technology plan will serve as a framework when aligning the MCPS technology plan.

- **Goal 1:** Provide a safe, flexible, and effective learning environment for all students.
- **Goal 2:** Engage students in meaningful curricular content through the purposeful and effective use of technology.
- **Goal 3:** Afford students with opportunities to apply technology effectively to gain knowledge, develop skills, and create and distribute artifacts that reflect their understandings.
- **Goal 4**: Provide students with access to authentic and appropriate tools to gain knowledge, develop skills, extend capabilities, and create and disseminate artifacts that demonstrate their understanding.

- **Goal 5:** Use technology to support a culture of data-driven decision making that relies upon data to evaluate and improve teaching and learning.

A detailed action plan with specific objectives and strategies is provided for each of these goals, with emphasis on the alignment of the Manassas City Public Schools' technology plan to their strategic plan, individual school improvement plans, and the Educational Technology Plan for the State of Virginia. The plan includes a timeline, resources or projected funding, assessment, and an appendix with local technology policies and guidelines.

The first technology plan focused on procuring equipment in order to meet state standards, and the training of teachers and students in the use of the equipment. The 2009-2013 technology plan focused on the integration of technology into instruction, data-driven decision making, continued professional development and enhanced communication, which will benefit all stakeholders.

A critical area of concern is future needs/replacement of equipment, increasing the bandwidth and how to ensure that fiscal support is addressed during budgetary planning. The realization of future needs is an ongoing and significant process and will be incorporated into future division technology advisory committee meetings to ensure that concerns of all stakeholders are addressed. The plan will also directly correlate to the Superintendent's Comprehensive Strategic Plan.

Process

The Technology Plan Overview

Jennie Dean Elementary Schools Comprehensive Plan (2011-2016), drives the continuous improvement work of the Division.

Mission Statement

The faculty and staff of Jennie Sean Elementary believe that

- Each child is a valued individual with unique physical, personal, social, emotional, and intellectual needs.
- Each child learns, achieves, and succeeds in different ways and at varied rates given developmentally appropriate academic goals.
- Teachers, staff, parents, and the community share the responsibility for implementing the school's vision and educating each child to their full potential.
- Each child learns to make appropriate choices in a safe, secure, supportive, and challenging environment.
- Positive relationships are the catalyst for the academic success of each child.

Vision
Each student will achieve his or her maximum potential as a productive citizen of the 21st century.

This plan establishes objectives and strategies to empower stakeholders to use technology in order to exercise options with content, process, products, and learning environments. Empowered students will be able to take ownership of their learning by engaging in inquiry, creativity and problem solving, on tools that are available within the school day, in every building. Technology plays a fundamental role in achieving our vision and preparing our students for the 21st century.

Strategic Goal
The ultimate goal for Jennie Dean Elementary Schools is the graduation of every student with the knowledge and skills needed to successfully enter post secondary education or the work force.

Jennie Dean Elementary School Strategic Objectives
1. All teachers will engage every student in meaningful, authentic and rigorous work through the use of innovative instructional practices and supportive technologies that will motivate students to be self-directed and inquisitive learners.
2. Jennie Dean will improve achievement for all students while closing the achievement gaps for identified student groups through an analysis of their own school data.

3. Jennie Dean will develop and implement a balanced assessment system that accurately reflects student demonstration and mastery of MCPS outcomes for student success.
4. Jennie Dean will create opportunities for parents, community, and business leaders to participate as actively engaged partners in supporting student achievement and outcomes for student success.
5. Jennie Dean will be accountable for developing essential leader, teacher and staff competencies and optimizing all resources to achieve the division's strategies goal and outcomes for student success.

Organization of the Plan and Work of the School Technology Advisory Committee

The Technology Advisory Committee, whose purpose is to address division technology issues and support each school's technology program through research, training, innovation, and collaboration. Dean's Technology Advisory Committee consists of staff members, and ITTS (Instructional Technology Training Specialists).

Timeline

Fall 2007- Division Technology Advisory Committee developed a vision in strategy for technology planning.

Fall to Spring 2007 – 2008 – Subcommittees headed by ITTS were formed to develop strategies to align with state goals and objectives.

Spring 2008 – The Division Technology Advisory Committee received and reviewed the draft of the technology plan.

June 2009 – The 2009-2013 MCPS Technology Plan was submitted to the School Board for approval.

Summer 2009 – The 2009-2013 MCPS Technology Plan was submitted to VDOE for approval.

Fall 2010 – Work began on revision of MCPS Technology Plan to align with new state technology plan/goals and objectives.

Winter 2011 – Draft presented to Division Technology Advisory Committee for review.

Spring 2011 – Revisions made and submitted.

Determining Our Needs

Members of the Manassas City Division Technology Advisory Committee were tasked with developing an assessment to measure the current strengths and weaknesses of technology integration in our division. All Dean staff members were then provided an opportunity to offer input regarding technology and how it is used in the school system. Progress will be reviewed and the survey will be modified and conducted on a yearly basis, in order to assess the progress of technology integration.

The results were analyzed and the main areas of concern emerged from various category groups.

Strengths:

- Dean has been successful in providing teachers with the educational training opportunities needed to become competent and proficient when using instructional technology to help student learning.
- Students are engaged in and excited about learning when technology is incorporated into their learning.
- Students are encouraged to use current technologies when completing assignments.
- Student to computer ratio meets the mandated number.

Weaknesses:

- Professional development opportunities need to be provided on a continuous basis.
- Teachers feel that they need more time to practice or develop their new technology skills.
- The division's infrastructure or Internet access needs to be increased to support instructional and administrative needs.
- A definitive replacement plan must be developed.
- While data required to support instructional planning is available, it is presently not in a format or delivered by means of a user- friendly interface that makes this wealth of information easily accessible and useful to teachers and administrators.
- There is a need for an improved system of communication for all stakeholders.

Recommendations:

- Increase Internet infrastructure.
- Increase professional development opportunities for all administrative and instructional staff.
- Increase partnerships with businesses in the area.
- A needs assessment must be conducted on a yearly basis and necessary adjustments to the technology plan will be made as needed.
- Replace all the old computers to support the SOL test and MAP testing
- Assess and make adjustments to the Internet Safety program on a yearly basis.
- Increase student and instructional staff awareness of the Acceptable Use Agreement and copyright practices.
- Provide one Instructional Technology Training Specialist (ITTS) for Dean, to capitalize technology investments and yield better learning opportunities for all stakeholders.

Deployment Process for the Plan

Once approved by the Principal, the Dean Technology Plan will be submitted to the Coordinator of Instructional Technology who will present it to the School Board. The plan will be made available to the community via the webpage. A copy will be held in the library for the community and all faculty members will be emailed a copy.

Actions

State Goals and Objectives with Local Strategies and Measures

Goal 1: Provide a safe, flexible, and effective learning environment for all students
Objective 1.1: Provide the technical and human infrastructure necessary to support real, blended, and virtual learning environments.

Strategies	**Measure/Evaluation Strategies**
1. Meet the Standards of Quality staffing requirements.	Documentation of actual count matching the one ITTS per 1,000 students' guideline.
2. Meet or exceed state infrastructure standards necessary to participate in on-line SOL testing.	Maintain district connection to the Internet and the fiber Wide Area Network connecting all MCPS facilities. Work with Central office Network administrators to maintain Internet service that allows for appropriate speed and redundancy. **Working Technology department chair to Develop process to evaluate existing hardware standards and to review needs for additional instructional technology hardware purchases.**
3. Provide opportunities for professional development that supports student and teacher learning.	Provide a variety of effective professional development options for instructional staff, including workshops, coaching and online instruction, surveys conducted, resources made available, etc. Increase embedded professional development opportunities for teachers within the school day and frequency of ITTS work with teachers on integrating technology. Design professional development opportunities with department chairs/team leaders that focus on content and collaboration. Maintain a program for instructional leaders that fosters effective use of technology in support of teaching and learning. Provide instructional leaders (administrators, directors, coaches, specialists) learning opportunities that identify effective practices. Provide opportunities for students, teachers and community to provide feedback regarding technology resources

	Offer professional development for all new teachers at the beginning of the year.
4. Provide instructional staff the technology resources to support a rich learning environment Continue to evaluate current infrastructure to meet the needs of 21st Century Learners.	100% of the recommendations are implemented or addressed in budget initiative. It is essential that we provide our students and staff with reliable equipment that is appropriate to the tasks at hand. Hardware, software, and on-line subscriptions consume the largest portion of the Instructional Technology budget. Standardizing the purchase and allotment of equipment best allows us to satisfy budgetary constraints, project budgetary requests while meeting the needs of our students, teachers and staff. . Dean school will provide necessary hardware including iPads, kindle fire, tools. Provide online subscriptions including research databases and access to a content management and collaboration system
5. Increase the number of interactive classrooms at all levels.	The increase of interactive classrooms in each building. A special emphasis will be placed on Smartboards and iPad usage and incorporation within the curricula.
6. Provide wireless access to the Internet and network at all MCPS facilities.	Improved wireless access.
7. Maintain, update and replace all desktops, laptops, projectors, interactive white boards, printers and servers and similar networkable devices.	The percentage displayed in our TrackIt inventory system.(Replacement Plan) and school-based inventory systems. Label all hardware and take thorough inventory of equipment. Dispose of unwanted/surplus equipment.
8. Ensure all virtual courses are accessible to students and staff members outside of school.	The guaranteed access to virtual courses. Support participation in online courses to address student and faculty needs.

Objective 1.3: Provide high-quality professional development to help educators create, maintain, and work in a variety of learner-centered environments.

Strategies	**Measure/Evaluation Strategies**
1. Provide high-quality professional development to help educators create, maintain, and work in a variety of learner-centered environments (ie. Schoolnet, PD360, Virtual Learning Environment, Beginner Teacher Induction Program).	Evidence of participation in the use of learner-centered environments. Evaluate how professional development enhances and supports student learning by using data to inform and guide professional development programs.

	Make sure all teachers are fully trained with how to use PD360, and train those teachers that are not.
2. Continue to partner with George Mason University for cohorts (ie. Reading Endorsement, ESOL Endorsement).	The number of teachers participating in cohort programs.
3. Continue to offer on-line courses focusing on technology infusion strategies and the development of teachers' and administrators' 21st century skills through North Tier, Smart Professional Development and other public/private/nonprofit partnerships.	The number of teachers participating in the North Tier online courses, other partnered institutions, and Smart Technology PD Program. Connect teacher and staff with online courses and webinars provided by outside organizations such as North Tier. Make sure proper advertisement of these courses is utilized.
4. Support innovative projects to help educators better understand the impact of new and emerging technologies on the learning environment and develop strategies to infuse them effectively into schools.	Evidence of innovative projects being conducted at the building level (i.e. iPads, Kindles, iPod Touch, Nooks, etc.) Provide special education department with iPads and libraries with the Kindle Fire.

Goal 2: Engage students in meaningful curricular content through the purposeful and effective use of technology.

Objective 2.1: Support innovative professional development practices that promote strategic growth for all educators and collaboration with other educators, content experts, and students.

Strategies	Measure/Evaluation Strategies
1. Provide differentiated professional development and training for educators and leaders on virtual learning environments (such as MOODLE, Schoolnet and PD360 user groups), the meaningful use of technology and data driven decision making.	Evidence of professional development offerings such as PD360, PLC meetings, and Schoolnet users group.
2. Provide opportunities for the development and delivery of professional development that focus on effective technology use.	Documentation of opportunities provided through MOODLE or traditional professional development offerings.
3. Develop the capacity for virtual student work and projects.	Number of users trained and number of hosted sessions.

Objective 2.2: Actualize the ability of technology to individualize learning and provide equitable opportunities for all learners.

Strategies	Measure/Evaluation Strategies
1. Provide reasonable access to Internet-connected devices that offer students the flexibility to learn anytime, anywhere.	Evidence of access to devices that allow flexibility to learn anytime, anywhere (ex: mobile labs, computer labs, iPad and Nook access, etc.)
2. Identify, develop, disseminate, and maintain resources to support teaching and learning using Schoolnet Align.	Continue to monitor use of Schoolnet.
3. Provide resource and support for Instructional Technology Training Specialists to assist teachers in integrating technology into teaching and learning.	Number of workshop agendas, ITTS Logs, and number of technology integration related conference attendance. There will be a monthly newsletter updating teachers on the latest technology they can use in their classrooms. Publish important and useful links on the school website.
4. Identify and disseminate information and resources to assist schools in evaluating the interactive and universal design features of hardware, software, and Internet sites to improve instruction and develop students' 21st century skills.	Evidence that schools evaluate various hardware, software, and Internet resources in an effort to improve instruction and develop students' 21st century skills. ITTS provided resources on school web pages.
5. Identify and disseminate information and resources to assist schools in identifying, obtaining, and maintaining the proper assistive technology needed to meet the needs for all students.	The dissemination of Assistive Technology (AT) information and resources that are available and the utilization and maintenance of these technologies to be evidenced in the form of student caseload files, Individualized Education Plan (IEP) accommodations and AT inventory of technologies under the direction of the AT Coordinator. (use Schoolnet data to help identify and disseminate this information)

Objective 2.3: Facilitate the implementation of high-quality Internet safety programs in schools.

Strategies	Measure/Evaluation Strategies
1. Identify and disseminate best practices and resources to promote the integration of Internet safety and security throughout the curricula.	Evidence of the integration of Internet Safety throughout the curricula, broadcasts and newsletters. Incorporate Internet Safety lessons and film projects into the Character Counts program in the elementary schools.

	Broadcast Public Service Announcements on internet safety on school programs Identify student work samples that demonstrate mastery of computer technology
2. Monitor the implementation of Internet safety policies and programs and provide technical assistance and support to ensure that schools have effective programs and policies.	Documentation on the status of the Internet Safety programs conducted in each building. Monitor the number of staff and teachers that have completed the necessary safety programs.
3. Provide resources and support for our school stakeholders to assist in ensuring Internet safety.	Number of Internet Safety websites, workshops, and resources made available. Provide students with internet safety sessions, flyers, posters, etc.
4. Monitor and implement Acceptable Use Policy for both staff and students.	Documentation of signed AUP for all staff and students.
5. Require Internet Safety certification through iSafe for staff.	Completion of iSafe certification and documentation in PD Express.
6. Provide a system to disseminate Internet Safety information to the community including parents and business members.	Documentation of detailed information provided to the community (ie. website, booklets, Parent Night/PTA/PTO, Potomac Nationals Internet Safety Night participation).

Goal 3: Afford students with opportunities to apply technology effectively to gain knowledge, develop skills, and create and distribute artifacts that reflect their understandings.

Objective 3.1: Provide and support professional development that increases the capacity of teachers to design and facilitate meaningful learning experiences, thereby encouraging students to create, problem-solve, communicate, collaborate, and use real-world skills by applying technology purposefully.

Strategies	**Measure/Evaluation Strategies**
1. Identify and disseminate information and resources that help schools provide ongoing, personalized, and just-in-time professional development for teachers implementing technological and pedagogical innovations.	Monitor professional development offerings and evaluate to determine if this strategy is being accomplished. Hold regular professional development sessions to determine teacher progress.
2. Enhance curricula using Internet resources and software that encourage creativity, collaborations, and problem solving.	Evidence of available software and Internet resources. Current listing of available websites, as provided by each ITTS.
3. Promote the safe and responsible use of social media.	Evidence of training and discussions on social media dangers integrated into curriculum as well as through training via Internet sites,

	school-based technology and parent nights, and other public events.

Objective 3.2: Ensure that students, teachers, and administrators are ICT literate.

Strategies	Measure/Evaluation Strategies
1. Ensure all teachers and administrators are TSIP certified.	Completion of TSIP/TSIP certification documentation and maintenance of division spreadsheet. Make sure it is regularly updated.
2. Provide and support high quality professional development through school-based ITTS focused on the acquisition and application of ICT skills for teaching, learning, and school management.	Observations through professional development offerings that focus on the acquisition and application of ICT skills for teaching, learning, and school management.
3. Ensure all teachers and administrators are aware of the state ICT skills as applicable.	Documentation posted on Schoolnet Align and school websites.

Objective 3.3: Implement technology-based formative assessments that produce further growth in content knowledge and skills development.

Strategies	Measure/Evaluation Strategies
1. Continue implementing Schoolnet Assess.	The number of school-based and division-based benchmark assessments administered via Schoolnet Assess. Train teachers on how to use SchoolNet to create benchmark tests at the end of every unit for gauging student progress.

Goal 4: Provide students with access to authentic and appropriate tools to gain knowledge, develop skills, extend capabilities, and create and disseminate artifacts that demonstrate their understanding.

Objective 4.1: Provide resources and support to ensure that every student has access to a personal computing device.

Strategies	Measure/Evaluation Strategies
1. Strengthen the capacity to support student use of personal computing devices at school.	Number of devices with access to the Internet. Availability for students to access these devices.
2. Provide opportunities for students to learn and apply ICT skills in school settings using a variety of authentic tools.	Description of how and the extent to which MCPS provides students with opportunities to learn and apply ICT skills.
3. Provide tools that extend students' capabilities customized to meet individual needs/differentiated learning styles, and	Evidence of how personal computing devices are customized and how options for customization support learning. Develop

support learning including assistive technology.	activities using personal computing devices that appeal to a variety of learning styles.

Objective 4.2: Provide Technical and pedagogical support to ensure that students, teachers, and administrators can effectively access and use technology tools.

Strategies	**Measure/Evaluation Strategies**
1. Continue to improve the network infrastructure to ensure that it can accommodate future increases in use of technology computers/tools.	Increased capacity and availability of network resources, including data ports, wireless availability, bandwidth, data storage, etc.
2. Provide and support high-quality professional development to assist educators in evaluating and integrating technology tools in ways that foster effective student use.	Provide monthly training schedule for group or individual training sessions before, after, and during the school day and document high-quality professional development offerings that help teachers integrate technology.
3. Provide ongoing just-in-time support to assist teachers in effectively integrating a variety of technology-based tools into teaching and learning.	Evidence in ongoing ITTS logs (documentation of types of support provided daily)
4. Provide timely and effective technical support to ensure that all tools and the network that supports them are installed and maintained properly.	Technology Work Order documentation.
5. Meet or exceed the SOQ staffing requirements.	One ITTS per 1,000 students.

Objective 4.3: Identify and disseminate information and resources that assist educators in selecting authentic and appropriate tools for all grade levels and curricular areas.

Strategies	**Measure/Evaluation Strategies**
1. Identify and disseminate information about new and emerging technologies.	Provision of information on school based websites, networks, and newsletter.
2. Design and implement pilot projects to evaluate a variety of personal computing devices.	Documentation of pilot projects that are being conducted. Provide evidence of student work on website and on display throughout school.
3. Provide a software review process in which technology staff ensures effective operability and quality instruction.	Number of requests staff completes. Conduct a yearly survey of software most used and reviews of software by teachers to ensure feedback.

Goal 5: Use technology to support a culture of data-driven decision making that relies upon data to evaluate and improve teaching and learning.

Objective 5.1: Use data to inform and adjust technical, pedagogical, and financial support.

Strategies	Measure/Evaluation Strategies
1. Evaluate current systems using tracking software such as TrackIt to identify gaps and overlaps	TrackIt semi-annual report
2. Evaluate funding for systematic replacement of existing technology to continue compliance with requirements for computers for online testing.	Five/seven year replacement plan
3. Evaluate need for grant application, use of e-rate and budgeting to ensure the deployment of new technologies and innovative projects.	Analyze annual needs assessment and budget to locate deficits
4. Continue evaluating effective use of Schoolnet/PowerSchool to ensure implementation of a "Virginia Compliant" SIS system.	100% of all project milestones will be delivered on-time.

Objective 5.2: Provide support to help teachers disaggregate, interpret, and use data to plan, improve, and differentiate instruction.

Strategies	Measure/Evaluation Strategies
1. Use Schoolnet Account and Assess to disaggregate, interpret, and use data to plan, improve, and differentiate instruction	1.Increased usage of assessment tests and variety of assessments 2.Evidence of discussions at each school on Data Days 3.Evidence of use of Account for creating groups for acceleration and intervention 4.Evidence of use of data when scheduling students for courses each August

Objective 5.3: Promote the use of technology to inform the design and implementation of next generation standardized assessments.

Strategies	Measure/Evaluation Strategies
1, Use Schoolnet Assess	The creation and number of benchmark tests, school benchmark tests, assimilation tests, and individual teacher tests.
2. Work with Schoolnet to implement next generation standardized assessment improvements	Record of number and item requests made to Schoolnet.

3. Work with Schoolnet to set up additional training	Number and type of training sessions. Make sure each teacher is aware of how to use SchoolNet by providing monthly training sessions.

Appendix 1:

Jennie Dean School Internet Safety Program

In March, 2006, The General Assembly of Virginia passed House Bill 58 (amended Section §22.1-70.2 of the Code of Virginia) that included a component requiring all schools in Virginia to file (every two years) an acceptable use policy (AUP) with the Superintendent of Public Instruction that prohibits division employees and students using division computer equipment for viewing, sending, receiving or downloading illegal material via the Internet. It furthermore specifies that schools must prevent access by students to material that the school division deems to be harmful to juveniles and that each school system select a technology for the division's computers having Internet access to filter or block Internet access through such computers to child pornography and obscenity. Schools must establish appropriate measures to be taken against persons who violate the policy. Schools must also include a component on Internet safety that is integrated in a division's instructional program. This policy may include such other terms, conditions, and requirements as deemed appropriate, such as requiring written parental authorization for Internet use by juveniles or differentiating acceptable uses among elementary, middle, and high school students.

Manassas City Public Schools has had an Acceptable Use Agreement in place and has been providing Internet safety training and information for staff, students, parents, and community stakeholders. MCPS realizes that because of the rapid growth of the Internet and the characteristics of our students, annual evaluations and updating of the program and training must and does occur. To further our effort to provide relevant Internet safety information for our students, MCPS is constantly striving to provide resources and training for all stakeholders in our learning community.

Roles and responsibilities of "all stakeholders" are listed in the Internet Safety Plan below and are adjusted annually, as necessary.

Safety measures are in place, including filtering and monitoring procedures. in accordance with §22.1-70.2 of the Code of Virginia, which filter or block Internet access through MCPS computers to such sites as child pornography as set out in §18.2-374.1:1 of the Code of Virginia and obscenity as defined in §18.2372 of the Code of Virginia.

If a staff member finds a site that is found to be educationally sound and would benefit instruction, there is a process in place to request that specific sites be unblocked. After submitting the request form, it is reviewed by the appropriate department and if found to be acceptable for student use the site is then released.

It is the policy of the City of Manassas Public Schools to protect computing resources under its management from unauthorized access, use, modification, copying and destruction. MCPS will take appropriate disciplinary action against any person who breeches this policy. Such action may include revocation of use privilege, or dismissal for staff members, or student suspensions. The action depends on the severity of the violation.

The Virginia Department of Education requirements for Internet safety training for students are:

1. The Internet is a powerful tool that should be used wisely.

a. The Internet allows students access to a vast library of previously unavailable resources.

b. The Internet enables students to communicate with people around the world.

c. The Internet provides a creative outlet for students skilled in writing, art, music, science, mathematics, and other topics.

2. Students need to know that not all Internet information is valid or appropriate.

a. Sexually explicit material or violent images can affect students negatively.

b. Sexual predators will try to convince students to trust them.

c. Internet information may promote negative attitudes, such as hate or intolerance, and dangerous or illegal activities, such as self-injuring behavior, gambling, and illegal drug use.

3. Students should be taught specifically how to maximize the Internet's potential while protecting themselves from potential abuse.

a. The critical-thinking skills students learn in the classroom, library, and lab should be applied to Internet resources and Web searching.

b. Students need to know what to do and who to ask for help when they encounter a person or site on the Internet that is offensive or threatening to them.

c. Students and adults are required by law to report illegal Internet communications and activities to Internet Service Providers and local law enforcement authorities

4. Internet messages and the people who send them are not always what or who they seem.

a. People in chat rooms, instant message "buddies," or those who visit a blog or wiki may not be who they appear to be. Students should learn to recognize when someone is potentially dangerous.

b. Students need to realize when an Internet encounter may be questionable and how to protect themselves when this occurs.

c. E-mail can cause malicious code- infection problems for a computer or network. Students should not open e-mail or attachments from unknown sources.

d. Students need to know which information is safe to share with others online, which should never be shared, and why sharing it could put them at risk.

e. Students never should reveal online any information about where they live or attend school.

f. Students need to be aware their electronic messages, even those with known friends, can leave electronic footprints that can be misused by others.

5. Predators and cyberbullies anonymously use the Internet to manipulate students. Students must learn how to avoid dangerous situations and get adult help.

a. Sexual predators deceive students by pretending to be students themselves. They sometimes lure young people into a false sense of security or blind trust and try to alienate them from their families. Students need to learn about these types of psychological ploys and how to get immediate adult help.

b. Bullies use Internet tools, such as instant messaging and the Web, to harass or spread false rumors about students. Students need to know how to seek proper help in these potentially dangerous situations.

c. Students need to know that posting personal information and pictures can allow predators to contact and begin grooming them for illegal meetings and actions. Personal photos can be easily misused or altered when posted on the Internet.

6. Internet activities, such as playing games and downloading music or video files, can be enjoyable. Students need to know which activities are safe and legal.

a. Gaming sites can attract sexual predators and/or cyberbullies.

b. Some games may contain pornographic and/or violent images. Students need to talk with parents about what is acceptable.

c. Students need to know how to detect whether a specific file download is legal and/or free of malicious code.

Roles and Responsibilities:

In order to ensure consistent Internet safety Manassas City Public Schools believes that it is important for "all stakeholders" to assume specific roles and responsibilities. These are in the detailed Internet Safety Plan below and as defined in the following regulations: Regulation 5-33 Personnel and Regulation 7-60 Students.

Role	Responsibility
School Board	- Understand that the Internet is constantly changing - Understand the educational advantages of the Internet - Stay up-to-date on vulnerabilities and legal issues related to the Internet

	and school responsibilities - Ensure that policies and procedures are in place for crisis management - Ensure communication with and among stakeholders for safety and security policies to be effective
Administrators	- Complete iSafe on-line certification - Enforce AUA and respond to any cyberbullying claims - Guide the implementation process of the Internet safety program - Understand that the Internet is constantly changing - Ensure that policies and procedures for crisis management are in place - Ensure that parents and students are aware of potential dangers - Make sure staff is monitoring students and covering Internet safety curriculum - Know how to check a computer's Internet history - Ensure implementation of Internet Safety Tips - Ensure that Internet use is age appropriate
Teachers (As mandated by the Virginia General Assembly, ALL K-12 teachers are required to integrate Internet Safety into their curriculum)	- Complete iSafe on-line certification - Enforce AUA and respond to any cyberbullying claims - Be aware of inherent Internet dangers - Monitor student Internet use - Report AUA violations to administrators - Integrate Internet safety into curriculum - Be familiar with and monitor copyright and ethics violations - Monitor students' use of the Internet by consistently circulating around the classroom - Know how to check a students' Internet history

	- Integrate Internet Safety Tips into daily instruction - Ensure that Internet use is age appropriate
Instructional Technology Training Specialists	- Complete iSafe on-line certification - Coordinate Internet Safety program for all stakeholders - Enforce AUA and respond to any cyberbullying claims - Ensure staff completes iSafe on-line certification - Provide introductory iSafe training for staff - Collaborate with teachers on proper monitoring of students and inherent danger awareness - Provide resources to teachers on Internet safety and Internet Safety Tips for daily instruction - Ensure that Internet use is age appropriate
Library Media Specialists	- Complete iSafe on-line certification - Be aware of inherent Internet dangers - Be familiar with and report all claims of cyberbullying - Reinforce Internet safety during library orientations - Monitor student Internet use in the library - Train teachers and students and offer resources on copyright - Ensure that Internet use is age appropriate
Computer Lab Teachers/Instructional Assistants	- Complete iSafe on-line certification - Be aware of inherent Internet dangers - Be familiar with and report all claims of cyberbullying - Reinforce Internet safety during Computer Lab instruction - Play a key role in conveying information to students and staff regarding cyberbullying, Internet predation, legal ramifications of online behavior

	and general advice regarding safe models for Internet behavior - Know how to check a students' Internet history - Integrate Internet safety into curriculum - Be familiar with and monitor copyright and ethics violations - Monitor students' use of the Internet by consistently circulating around the classroom - Ensure that Internet use is age appropriate
School Resource Officers	- Complete iSafe on-line certification - Respond to violations of AUA that involve illegal acts - Play a key role in conveying information to students and staff regarding inherent dangers, cyberbullying, Internet predators, legal ramifications of online behavior and general advice regarding safe models for Internet behavior - Be familiar with and monitor Internet safety allegations - Ensure that Internet use is age appropriate
School Counselors	- Complete iSafe on-line certification - Be aware of inherent Internet dangers - Be familiar with and report all claims of cyberbullying - Speak to students about the potential risks on the Internet and how to handle those situations properly - Inform parents and students about relevant MCPS technology regulations (AUA, the technology portion of the student code of conduct, specific school guidelines, privacy regulations) - Offer additional resources to students on Internet safety and cyberbullying - Ensure that Internet use is age appropriate
Network Administrators	- Monitor network and Internet at administrator's direction

	- Report any known AUA violations to administration - Work with administration to block known harmful sites beyond the applied filter - Ensure that Internet use is age appropriate
Instructional and Administrative Technology Supervisors	- Maintain filtering technology for all Internet traffic - Provide training as necessary to administrators and technical staff - Ensure that Internet use is age appropriate - Serve as a liaison between VDOE and the division
Students	- Abide by the Acceptable Use Agreement and the Student Code of Conduct - Report AUA violations by other students to the administration - Report instances of cyberbullying to the administration - Learn and understand the dangers of the Internet, strive to be safe when online, and know when to get adult help - Understand that not all Internet information is valid or appropriate - Understand that Internet message and the people who send them are not always what or who they seem - Know which activities (games, downloading music or video files) are safe and legal
Parents, Grandparents, and Caregivers	- Understand that the Internet is a valuable learning, communication, and entertainment provider. - Understand the potential Internet dangers and discuss with their children. - Provide protection for their children. - Monitor their child's Internet use.

Roles and responsibilities will be reviewed in May of each school year for any needed adjustments.

Filtering and Monitoring Procedures:

Check Point Firewall - Provides security and protection for inbound and outbound traffic to/from the Internet. MCPS uses CheckPoint Firewall for its firewall system. Rules are based on services needed by school resources. Rules for inbound traffic to certain MCPS servers are limited to only those services needed (example - SMTP & HTTP). Rules for outbound traffic are also limited to only necessary sevices. All inbound/outbound traffic is logged and reviewed by the LAN/WAN Administrator on a weekly basis. Rules are adjusted based on needed services or issues found.

LightSpeed Systems Total Traffic Control System – Provides additional network security for inbound and outbound traffic. Contains a filtering system for controlling access by staff and students to undesired or dangerous web sites. Web sites are placed into categories based on site content. Categories can be blocked or allowed based on MCPS standards. A subscription service provides updates to the categories on a daily basis, as well as, a reporting system for tracking Internet usage.

Data and Network Security:

Data and Network Security is handled by the Administrative Technology Department. Network infrastructure is secured through the use of VLAN's and network monitoring. Data resources are backed up on a daily basis and industry standards are utilized.

Users are only allowed access to those network resources that are required to perform their jobs and/or are instructionally necessary. Employees should not use electronic mail for confidential matters or privileged communications, such as student education records, unless appropriate measures are taken to ensure confidentiality and to maintain the appropriate privilege. Employees shall adhere to all school, School Division, state and federal laws, policies and standards including the Family Education Rights and Privacy Act (FERPA).

Procedures to Address Breach of Security and/or Safety:

Inappropriate use, security and safety breaches are handled at the school level following the appropriate chain of command starting with notification of a staff member, referral to building administrator and possible involvement of the School Resource Officer. These breaches are dealt with by using the guidelines in our AUP and Student Code of Conduct.

All major security and safety breaches are referred to and handled at the district level by the technology departments in conjunction with the Superintendent. If the breach violates local, state or federal laws, appropriate agencies will be notified. Major breaches are those that might include loss of service or loss of data.

The use of computer resources is a privilege, not a right. Misuse of Internet access or a violation of this regulation may result in the account or the user's access privilege being denied, revoked or suspended. Penalties may result in disciplinary action up to and including suspension or expulsion, formal reprimand, or dismissal, as well as, potential civil or criminal liability and prosecution.

Documentation of any such incident is kept by the Department of Administrative Technology. If student discipline is involved, documentation is kept at the school level as well. If staff discipline is involved, documentation is kept by the Human Resources Department.

Professional Development/Informational/Outreach Programs:

It is the goal of Manassas City Public Schools to provide training for all staff members, students, parents, guardians and community members emphasizing that monitoring students is crucial and that students need to hear the rules often.

Resources will be provided for use when covering the six instructional concepts with students:

1. The Internet is a powerful tool that should be used wisely.
2. Students need to know that not all Internet information is valid or appropriate.
3. Students should be taught specifically how to maximize the Internet's potential while protecting themselves from potential abuse.
4. Internet messages and the people who send them are not always what or who they seem.
5. Predators and cyberbullies anonymously use the Internet to manipulate students. Students must learn how to avoid dangerous situations and get adult help.
6. Internet activities, such as playing games and downloading music or video files, can be enjoyable. Students need to know which activities are safe and legal.

<u>For the Staff the Instructional Technology Training Specialists will:</u>

Monitor and assist with iSafe certification

Provide Broadcast/Daily Tips to be discussed in the classroom

Provide training detailing the specifics of the Acceptable Use Agreement using a PowerPoint presentation

Provide additional videos

Provide resources.

For Students the PTA/PTO, FBLA, ITTS, Library Media Specialists, Computer Lab Teachers/Assistants, SRO's and teachers will:

Provide Internet Safety Assemblies

Organize and run Poster Contests

Provide Broadcast/Daily Tips, which will then be discussed in the classroom

Conduct grade appropriate Internet Safety Surveys

Provide additional videos

Review availability of resources on individual school web pages and in newsletters

Provide continuous reinforcement about Internet safety, across the curriculum

For Parents/Community the PTA/PTO, Administrators, FBLA, ITTS, Library Media Specialists, Computer Lab Teachers/Assistants, SRO's and teachers will:

Provide opportunities for attendance at Internet Safety Assemblies/Informational Sessions

Provide ongoing access to Broadcast/Daily Tips

Provide PTA Programs with a variety of knowledgeable facilitators.

Provide access to additional videos

Provide additional resources on school and division web pages and in school newsletters

Evaluation:

The Coordinator of Instructional Technology is the primary source of contact and coordinates all division plans and programs related to Internet safety.

In May of each year the Department of Instructional Technology with the assistance of the School Technology Committees, Library Media Specialists, Computer Lab Teachers/Assistants, and School Resource Officers will conduct annual evaluation of the Internet Safety program. This annual evaluation will be accomplished in conjunction with the review of the division's technology plan.

Evaluation will cover, but not be limited to:

- Review of roles and responsibilities of individuals as related to the program

- Review data for security violations and how to prevent further breaches

- Review number of Acceptable Use Agreement violations for both students and staff

- Review comments from all stakeholders and analyze survey results to determine program changes that need to be made

- Review VDOE guidelines and state legislation as they relate to the MCPS program

Internet Safety Program Implementation:

2007

- Manassas City Public Schools updated and approved the Acceptable Use Agreement to include information relating to Internet safety in our schools.
- Committee of teachers and Instructional Technology Training Specialists worked on aligning the iSafe program with the Virginia standards and selecting supporting materials
- Acceptable Use Agreement reviewed for all students and staff
- Osbourn High School Resource Officer presented the Internet Safety/iSafe Program to the building administrators
- Osbourn High School SRO gave multiple presentations to the Peer Mentor classes (approximately 200 students) and certified students in the iSafe Mentor Assembly Program
- Osbourn High School SRO gave presentation to and certified Instructional Technology Training Specialists
- FBLA students were trained and certified as iSafe Mentors
- SRO lead, with the support of the Coordinator of Instructional Technology and FBLA students, preparations for creating a student Internet Safety Program utilizing the iSafe.org curriculum
- Internet Safety program for Manassas City Schools was launched with an assembly for 500 sixth graders at Mayfield Intermediate School. The program was sponsored by the Mayfield PTA.
- An Internet safety poster contest was conducted with the sixth graders. Prizes were provided by the Mayfield PTA for the top 3 student posters.
- The first parent program was presented at Metz Middle School
- The Library Media Specialists and computer lab instructional assistants participated in the iSafe.org online certification program.
- Osbourn High School FBLA students began working on Parent and Student Internet Safety presentations
- Mayfield Intermediate School PTA sponsored an Internet Safety program for approximately 25 parents. The program was prepared and presented by the High School SRO and FBLA Officers
- The Metz Middle School Library Media Specialist and Instructional Technology Training Specialist presented a program for all of the eighth graders

- Business Leadership students received certification in the iSafe Mentor Program and approximately 400 high school students were presented with segments of the iSafe curriculum with follow-up activities. FBLA students produced and filmed an Internet Safety video, created games and puzzles that will be used with K-6 students and developed a program to be used with seventh and eighth graders.

2008

- Business Leadership students received certification in the iSafe Mentor Program and approximately 400 high school students were presented with segments of the iSafe curriculum with follow-up activities. FBLA students produced and filmed an Internet Safety video, created games and puzzles that will be used with K-6 students and developed a program to be used with seventh and eighth graders.
- Instructional Technology Training Specialists and SRO from the high school, with input from across the division, reviewed the first year's progress and created the Internet Safety Program that will be used across the division.
- Coordinator of Instructional Technology met with each building administrator to discuss implementation of training/certification for all staff members.
- Osbourn FBLA students presented at the VBEA Conference held in Reston
- Submit Internet Safety Program outline to VDOE
- Acceptable Use Agreement Presentation for students and staff (staff- PowerPoint)
- Train and certify staff and administrators

2009

- Implement program across the division and to all stakeholders
- Evaluate program and Acceptable Use Agreement and make adjustments
- Each building facilitated how their Internet Safety Program was conducted.
- iSafe certification of new teachers and staff is ongoing to maintain 100% compliance.

2010-2011

- Use of the Professor Garfield's Infinite Learning, developed by the Department of Education and the Professor Garfield Foundation was implemented.
- Participation in the Internet Safety Night at Pfizer Stadium.
- Regularly monitor student folders for inappropriate files and file types.
- Periodically monitor website access to ensure sites are safe and secure.
- Made teachers aware of internet bypass techniques used by students (ie. proxy bypass, anonomizers and other techniques
- Used in-school TV broadcast to inform students regarding internet safety.
- Conducted Internet safety survey.
- Posted Internet safety guidelines in all computer labs.
- iSafe certification of new teachers and staff is ongoing to maintain 100% compliance.
- Began program with school newspaper to have monthly internet safety article.
- School broadcast used to post internet safety facts on a weekly basis.

- Tips are given to parents in the school newsletter.
- Made staff aware of new technologies pertaining to endangerment of their safety.
- Implemented cyberbullying awareness in both English and Spanish.
- Distributed NetCetera booklets and bookmarks regarding Chatting with Kids About Being Online.
- Display bulletin boards regarding Internet Safety.
- Osbourn High School newspaper posted articles throughout the year pertaining to such subjects as cyberbullying, etc.
- Sessions for students in the middle school were conducted bi-annually by the Library Media Specialists and Instructional Technology Training Specialists.

MCPS Internet Safety Suggested Curriculum

Grade	VA Internet Safety Guidelines and Topics	Curriculum Resources
k-2	Cyber Citizenship: 1b Cyber Security: 4b, 6c Personal Safety: 1a, 2a, 2b, 4d, 4e, 5b, 6b	My World and Internet Safety Surf Swell Island:Privacy Falls Faux Paws Internet Safety Who'S your Friend?
3-5	Cyber Citizenship, Cyber Citizenship and Online Safety, Cyber Community Issues, Cyberbullying, Safety Online, Safe Website Design, Safety in Online Gaming: 1a, 1b, 1c, 2c, 3a, 3b, 3c, 4c, 4d, 4f, 5a, 5b, 5c, 6a Cyber Security, Spam Scam Safety, Risks of Spyware, Acceptable Use Policies: 3a, 4b, 4c, 6c, 1a, 1c, 3a, 3b, 3c, 5b	Wizzy Wigs Surf Swell Island-Temple of Tact Garfield Cyberbullying Brain Pop Swell Island Virus Cave http://www.infinitelearninglab.org/ Surf Swell Island-Challenge of Doom http://pbskids.org/webonauts/

	Intellectual Property, Effective Outreach, Integrated Literacy: Internet Safety Focus, Personal Safety, Empowerment Challenge, Safety and Your Identity, Cyber Predator Awareness, Predator Identification, Text Messaging Safety, Creative Ownership and Copyright, Intellectual Property, Play it Safe Online, Web Logs – A Positive Approach to Blogging: 2a, 2b, 3a, 3b, 4a, 4b, 4c, 4d, 4e, 4f, 5a, 5b, 5c, 6a, 6b	http://websites.kahoks.org/safeweb/
6-8	Cyber Community Issues, Cyber Citizenship, Cyberbullying Negative Networking: A Look at Gangs Online, Cyber Security, Safe Website Design, Safety in Online Gaming: 1a, 1b, 1c, 2a, 2c, 3a, 3c, 4f, 5a, 5b, 5c, 6a, 3a, 4a, 4b, 4c, 4f, 6a, 6c Effective Outreach, Integrated Literacy: Internet Safety Focus, Literacy Review Cyber Harassment: 1c Intellectual Property: 3a Personal Safety, Online Personal Safety, Social Networking in Online Communities, Play It Safe Online, Legal Trends in Cyber Safety and Security, Web Logs – A Positive Approach to Blogging, Online Shopping Risks, Internet Life Skills Unit: 2a, 2b, 3b, 4a, 4b, 4c, 4d, 4e, 4f, 5a, 5c, 6a	This FBI site includes links to Internet Law Enforcement Stories and A Parent's Guide to Internet Safety. http://www.fbi.gov/fun-games/kids/kids GetNetWise offers links to educational and entertaining Internet sites that are appropriate for kids http://www.cybercrime.gov/rules/kidinternet.htm Cyber ethics for kids http://www.cybercrime.gov/rules/kidinternet.htm Interactive quizzes for kids and adults http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=714 Netsmart teens makes kids aware of internet dangers and safety http://www.netsmartz.org/index.aspx Free to educators, the CyberSmart! Student Curriculum empowers students to use the Internet safely, responsibly, and effectively. http://cybersmartcurriculum.org/lessonsbygrade/6-8/ The Virginia Dept. of Education has teamed up with the Professor Garfield Foundation and the Office of

	Predator Identification, Willing Participant: 3a, 3b, 3c, 5a, 5b, 5c	the Attorney General of Virginia to provide guidance for students, teachers and parents to help students protect themselves online. http://infinitelearninglab.org/ Webquest proving that you know how to be safe on the internet. http://roselle12.dupage.k12.il.us/education/components/scrapbook/default.php?sectiondetailid=86170&PHPSESSID=073d799d7346e435bbd0ce83f4cd4d5e Cybercitizenship guide to help increase your safety skills when you use digital technology. http://www.jmu.edu/iiia/webdocs/Publications/CyberGuide%20Ed%20FINAL.pdf Stop cyberbullying http://www.stopcyberbullying.org/index2.html
9-12	Cyber Community Issues, Legal Trends in Cyber Safety and Security, Online Gambling, Negative Networking: Terrorists, Gangs, Cults, Cyber Harassment: Bullying and Stalking Online, Pornography On the Web, Security: Cyber Citizenship, Online Freedoms and the Culture of Online Communities, Cyber Community Survey: 1a, 1b, 1c, 2a, 2b, 2c, 3a, 3c, 4a, 4b, 4d, 5a, 5b, 6a, 6b Cyber Security, Identity Theft, Cyber Security: Malicious Code, Homeland Security, Internet Life Skills: 3b, 3c, 4a, 4b, 4c, 4d, 4e, 4f Effective Outreach, Internet Life	Safe Internet Surfing Tips http://kidshealth.org/teen/safety/safebasics/internet_safety.html Federal Trade Commission - Social Networking Sites: Safety Tips for Teens and Tweens http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm Get Netwise – Safety By Age http://kids.getnetwise.org/safetyguide/age/14-17 Safe Teens http://www.safeteens.com/ Safety Tips for Tweens and Teens http://www.onguardonline.gov/topics/safety-tips-tweens-teens.aspx

	Skills, Service Learning Curriculum, Social Issues: 1c Intellectual Property, Copyright and Fair Use, Intellectual Property, Learn Before You Burn Lesson: 3a, 6c Personal Safety, Privacy and the Internet Online Privacy, Identity Theft, Legal Trends in Cyber Safety and Security Online Shopping Risks: 2a, 2b, 3a, 3c, 4a, 4d, 4e, 4f, 5c, 6a Predator Identification, Online Relationships, Cyber Relationships: 2b, 4a, 4b, 5a, 5c, 6a	Age Based Guidelines for Internet Use – Microsoft http://www.microsoft.com/protect/parents/childsafety/age.aspx NetSmartz Teens http://www.netsmartz.org/netteens.htm

Internet Safety Vocabulary

anti-virus: Software that protects a computer from malicious code.

attachment: A data file sent from one computer to another along with an e-mail or an instant message.

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

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

buddy list: Instant message addresses of favorite users. List enabled designated users to know when their "buddy" is online so that both can easily communicate.

bulletin boards: Message boards, public areas on the Internet where messages or comments can be posted for other board members to read and reply to.

chat rooms: These Web sites or online services facilitate electronic discussions by quickly posting the comments and responses of multiple users.

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

code: Written instructions in a computing language.

copyright: The exclusive rights to reproduce, publish, and sell things produced by the person who owns the copyright.

cyberbullies/cyberbullying: This refers to any online threats by one student toward another, typically through e-mails or on Web sites (e.g., *blogs, social networking* sites).

cybercrime: This refers to any Internet-related illegal activity.

cyberspace: Virtual Internet community in which real people interact through electronic means.

cybersecurity (sometimes *cyber security*): This refers to any technique, software, etc., used to protect computers and prevent online crime.

cyberstalking: This refers to a number of methods individuals use to track, lure, or harass another person online.

download: To copy information (data) from the Internet.

electronic footprints: Computers maintain a record of all Web site visits and e-mail messages, leaving a trail of the user's activity in cyberspace. These data can still exist even after the browser *history* has been cleared and e-mail messages have been deleted.

favorite(s): This is the name for *bookmarks* (see above) used by Microsoft's Internet Explorer browser.

file: The specific location of data within a computer record.

file extensions: The three or more letters at the end of a file name (e.g. .exe, .jpg, and .doc, etc.) defining the file "type", such as a text file, database file, or graphic file.

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

filter/filtering: This refers to different types of software that screen and block online content.

firewall: Set of related hardware and software programs designed specifically to protect a computer or computer network from unauthorized external access.

flame: To send a mean or hurtful electronic message.

gaming: This term describes Internet games, which can be played either individually or by multiple online users at the same time.

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

grooming: This refers to the techniques sexual predators use to get to know their victims in preparation for sexual abuse.

history: This is a tracking feature of Internet browsers that shows all the recent Web sites visited.

identifying information: Personal information that can be used by online predators to distinguish you from another person and possibly to find you in real life (e.g. name, gender, age, etc.)

identity theft: In this crime, someone obtains the 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.

IM-Instant Messaging: Real time Internet communication. A "private chat room".

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

intellectual property: Material protected by copyright laws including songs, movies, software, and books.

Internet safety: Being educated and empowered to take control of online experiences.

looping: Website code that does not allow a visitor to exit. Feature of may adult Internet sites.

malicious code: This refers to any computer code that is intentionally introduced into a system to damage or destroy files or disrupt the operation of a computer.

monitoring: This refers generally to the technique of tracking where people have been on the Internet by looking at the *history* of the browser. It also refers to software used for the same purpose.

netiquette: network etiquette; the do's and don'ts of online communication.

parental controls: Special features or software packages that enable restricted access to Internet sites.

P2P (see peer-to-peer computing) peer-to-peer (P2P) computing: This is a popular way for Internet users to share one another's computer files—usually music, game, or software files.

phishing: This scam involves sending a fraudulent e-mail soliciting credit card, Social Security, or other personal information from an unsuspecting user.

piracy: Theft to produce counterfeit copyrighted software and other material.

plagiarism: Stealing someone else's work and pretending it's yours.

posting: Placing a message or photo to an online message board or website.

screen name: Online name or nickname. An alias used in Cyberspace.

social networking: This refers broadly to online communities where people share information about themselves, music files, photos, etc. There are many social networking Web sites (e.g., MySpace, Facebook, or Friendster).

spam: This refers to any unsolicited e-mail, or junk mail. Most spam is either a money scam or sexual in nature. Internet Service Providers, e-mail software, and other software can help block some, but not all, spam.

spoof/spoofing: Fake e-mail messages or web pages mimicking those of legitimate business in order to trick you into providing personal information (identity theft).

spyware: This refers to a wide-variety of software installed on people'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*.

trojan horse: A malicious code that appears harmless yet launches a virus or worm.

URL: Defined as Universal/Uniform Resource Locator, is another name for a Web address. The URL is located at the top of a web page and generally begins with http://www.

viruses: These are software programs that typically arrive through e-mail 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 e-mails or *spam*.

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.

worm: Self-propagating computer virus embedded in a file.

Internet Safety Tips for Daily Instruction

Each classroom teacher is responsible for discussing and incorporating the Internet Safety Tips for Daily Instruction emphasizing them during lessons and activities across the curriculum. These tips will be part of each school's daily broadcast. They may be altered as deemed necessary by the age of the students. For additional help on effective ways to integrate Internet Safety, contact your ITTS or Media Specialist.

INTELLECTUAL PROPERTY/RESEARCH:

1. Choose search engines carefully. Some are specifically designed for kids, and others offer kid-safe options. For a safe and efficient search, use the search engine suggested by your Library Media Specialist. It will help you find reliable sources of information and distinguish fact from fiction.

2. When engaged in any online activity and you come across material that makes you feel scared, uncomfortable, or confused, immediately tell an adult.

3. It is illegal to share copyrighted materials without permission. Just because something is available online doesn't mean it is legal to copy, download, or use. 'If in doubt, always ask permission from the author.'

4. If you would like to copy something on a website, be sure that you follow proper procedures for using, downloading, redistributing, or reproducing. Most websites have a section that explains how you are allowed to use information from the site.

5. Be careful not to download files without permission. Users often do not know what they have downloaded until it's on their computers. Some files may contain harmful viruses or may affect the running of other programs on the computer. It is against MCPS regulations to download files at school.

6. When you illegally download, reproduce, or redistribute information, you risk legal action. Penalties may range from warnings and/or costly fines to jail time.

7. If download music without permission—whether it is one song or a hundred songs—you are violating copyright laws and run the risk of being sued. The Recording Industry Association of America led over 3,000 lawsuits against individuals since May 2004, resulting up to a $150,000 fine per copyrighted song.

8. Anyone can post anything on the Internet. Just because it is online does not mean it is true. Make sure it's true by following these tips:

a. Can you find the information on another trusted website or research database?

b. Does the website provide contact information and include an email address, phone number, and mailing address?

c. Does the website list the author's credentials?

d. Are there links to other reputable websites? Honest websites aren't afraid to link to other websites.

e. Did you know that websites in the educational domain (.edu) or news and nonprofit organizations (.org) are more likely to be honest?

9. Make sure you are using an updated website when conducting research**.** A medical website posting outdated medical information could be potentially harmful. Check to see when the page was last updated and make sure all the links are working.

10. Some websites may be biased such as those with advertising and banners, as they may be part of a hidden agenda.

11. When researching a topic that is controversial, look for informational websites with a fair and balanced point of view.

12. If you are looking for a specific website and do not know the exact URL, use the search engine. Do not type an unknown web address in the URL window.

13. By sharing files with others, you could unknowingly end up downloading and distributing harmful viruses. Make sure your anti-virus program is up-to-date at home.

14. Carefully check out file-sharing services. Make sure the services are not offering copyrighted material without the permission of the author or artist. Also check to make sure the sites do not offer inappropriate material.

15. Avoid copying and pasting web page text directly into your document with the intentions of later changing or using portions of the text. Copying and pasting text directly into your document from a website without changing or citing as a direct quote is plagiarism. Take notes in your own words!!

16. Always cite your online sources.

17. Take good notes when conducting online research. Write down the name of the author, title of the website, organization name, URL of the website you are using, and date you retrieved the information.

CYBER SECURITY - PASSWORD PROTECTION

18. Don't use passwords that are based on personal information that can be easily accessed or guessed. Avoid using the numbers in your birthday, social security number, phone number, or address.

19. Don't give out your password.

20. Don't use words that can be found in the dictionary of any language as your password. Hackers use special programs that crack passwords by scanning the dictionary. Instead, use a combination of letters, numbers, and special characters.

21. Develop a mnemonic or memory system for remembering complex passwords. For example use "Iltwfb" for I like to watch football.

22. Consider using different passwords for different types of accounts, and make sure you keep your password list in a safe place. Don't check the "remember my password" option when you are using a public computer.

CYBER SECURITY - GENERAL TIPS

23. Set your browser security to high. If this setting causes a website not to work properly, you can designate a Web site as trusted which will allow the site to work correctly under the High security setting. All of these controls can be set using Internet Options from the Tools menu.

24. Avoid pop-up windows that contain advertisements or offensive content by turning on your pop-up blocker. This prevents small additional windows from opening when you visit Web pages and can be turned on or off as needed. Pop up windows often contain viruses and spyware. It's important that you close the windows to avoid installing any of this on your computer.

25. Make sure you understand and are comfortable with the terms of the agreement before accepting an end-user license agreement when installing software programs at home.

26. It's not always safe to send personal information or make purchases over the Internet. These actions should not be done without parental permission. Make sure the site encrypts your transactions. Encryption prevents the attackers from being able to view the information.

27. If your computer is left connected to the Internet or if you operate on a wireless network that never shuts down, be sure you have firewall software for protection.

28. Remember to log off the Internet when you leave your computer.

29. Never share your user id with anyone except trusted adults.

30. Be sure to tell a trusted adult when someone on the Internet tries to contact you or makes you feel uncomfortable.

CYBER SECURITY - VIRUSES AND THREATS

31. Viruses are types of malicious codes that require you to actually do something before it infects your computer. This action could be opening an e-mail attachment or going to a particular web page. Always look out for suspicious e-mail and don't open e-mail from someone you don't know.

32. Worms are also types of malicious code that infect your computer without the user having to do anything. Worms typically start by attacking a software flaw. Once the computer has been infected, the worm will attempt to find and infect other computers via e-mail, websites, or network-based software. Always keep your anti-virus software up to date and keep up with latest patches for your operating system at home.

33. Some programs claim to be one thing while in fact doing something different. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder. Make sure you investigate the reputation of the program before downloading or installing it on your computer at home.

34. Never visit or use sites or networks that allow users to illegally download music or movies. By installing unauthorized copies of software applications, many "attackers" take advantage of this to spread viruses.

35. At home reduce the chances of getting infected by viruses by using anti-spyware tools or software programs that identify and remove spyware, a common source of viruses. Regularly scan your computer for spyware.

36. Firewalls prevent some types of virus infections by blocking malicious traffic before it can enter your computer. Trying to get around firewalls at school violates your AUA agreement. Remember that firewalls are there for your protection.

37. Anti-virus software and firewalls are important elements to protecting your information, however, neither of these are fool proof. Combining these safe-guarding technologies with good safety habits is the best way to reduce your risk.

38. If your home computer should become infected with a virus, change your passwords as your original passwords may have been compromised during the infection. Make sure your new passwords are difficult for attackers to guess.

39. Always back up your work to your web folder, CDs, DVDs, flash drives, and other storage media in case of a virus infection that may delete or compromise your data stored on the computer's hard drive.

ONLINE PERSONAL SAFETY - E-MAIL

40. If it sounds too good to be true, it probably is. Beware of e-mails that promise fantastic rewards or money. There are no wealthy strangers willing to send you money or gifts. These messages are most likely spam, hoaxes, or phishing schemes.

41. Don't advertise that you are away from your home. Some e-mail accounts offer autoresponder features that automatically send messages to anyone who e-mails you for a designated period of time.

42. Supplying your e-mail address to various websites and online organizations may increase the amount of spam you receive. Check out their privacy policy before you give out your address and any personal information.

43. Don't open any attachments from anyone unless they are run through an anti-virus program.

44. Don't reply to spam, harassing, or offensive e-mail or forward chain e-mail letters.

45. Do not forward chain e-mail communications. No chain e-mails are legitimate. Chain e-mails cannot bring you fortune or cause bad luck, they will not make you rich, and you will never get that free trip.

46. Phishing is an online scam used to commit identity theft. A fraudulent, but official-looking e-mail is sent to a user in an attempt to con that user into divulging personal and/or private information, which is then used for identity theft. Don't get caught!

47. Make sure that you are using the most up-to-date Internet browser software. More recent versions often offer enhanced security protection.

48. If you receive an email from someone you don't know, delete it.

49. Always work on the principle that your email could wind up on the front page of a newspaper. Some people have a habit of forwarding (without permission) emails to other friends and before you know it your personal views could be in the hands of thousands.

50. Think carefully about what you include in your subject line. If you use 'Hi', 'Good news' or 'Check this out', you can almost guarantee a large number of your messages will be marked as spam.

51. Always log off when finished with your e-mail communication. It's quick, easy and may save your account from unwanted trespassers.

52. Look closely at subject lines in e-mail messages. Spammers fake subject lines so they look like they are from friends. Some examples might be "Re: your mail", "How are you?", "Check this out", and "Thinking of You".

53. Avoid opening any e-mail attachments with the extensions .exe, .vbs, .shs., .pif, .scr, and double extensions. Delete any questionable e-mail before you open any attachments.

54. Spammers fake e-mail addresses from legitimate companies and place big warning messages in the subject line. They also do whatever they can to make the website or email look real.

55. Be careful how you word your e-mail messages and avoid giving specific details about your personal information.

ONLINE PERSONAL SAFETY - SOCIAL NETWORKING

56. When using social networking sites such as MySpace, set your profile to private so only those on your contact lists are able to view them. Public posting of profiles places your personal information for anyone to see and could put you at risk from those who wish to take advantage of such information.

57. Choose gender-neutral screen names or nicknames — such as your initials or a word. Make sure the name doesn't include information revealing your identity or location.

58. Use the privacy settings on social networking sites to restrict access to your "spaces" or blogs to only people you know.

59. Never give out personal information or arrange to meet someone in person whom you've met online without first checking with your parents.

60. If you receive an IM from someone you don't know, block the sender. Only IM people you know in person and whom your parents have approved. It is not a contest to see who has the

greatest number of contacts. Don't add new members to your lists unless you know who they are or you ask a parent.

61. Think before typing, "Is this message hurtful or rude?" What you post online stays online - forever! So thinkb4uClick! Don't do or say anything online you wouldn't say offline.

62. View the Internet as a book not a diary. Make sure you are comfortable with anyone seeing the information you post online. If you want the information to be private or restricted to a small, select group of people, the Internet is probably not the best forum.

63. Do not respond to any rude or annoying messages or ones that make you feel scared, uncomfortable, or confused. Depending on the seriousness and number of incidents, you may want to show these messages to your parents, teacher, or report them to the proper authority.

64. If you are being harassed or bullied online, tell a trusted adult immediately. Save an electronic copy and/or print a copy and report the incident(s) to a parent or school official.

65. Cyber bullying is considered a form of harassment in most states, is punishable by law as a misdemeanor, and in some cases a felony if it poses a reasonable threat to a one's personal safety. (Emphasize the severity and consequences of cyberbullying)

66. The United States Data Protection Act also upholds the right to keep personal information and records private. Depending on how personal the information is, posting someone's private and personal information on the Internet without permission can result in punishment by federal law.

67. Some sites and services ask users to post a "profile" with their age, sex, hobbies, and interests. While these profiles help kids "connect" and share common interests, potential exploiters can and do use these profiles to search for victims.

68. Beware of users who may pose as someone else — a different person or person of a different age — without others knowing. Such users have taken advantage of this to lure or exploit kids.

69. You can't "take back" the online text and images you've entered. Once online, "chat" as well as other web postings become public information. Many web sites are "cached" by search engines, making photos and text retrievable long after the site has been deleted.

70. Students have been punished by their families and schools; denied entry into schools; and even not hired because of dangerous, demeaning, or harmful information found on their personal sites or blogs.

CYBER COMMUNITY - POSTING PICTURES AND VIDEOS ONLINE

71. Only use webcams or post photos online with adult permission and/or supervision. When posting pictures or videos online, ask yourself if you would be embarrassed if your friends or family saw the pictures or videos you post online. If the answer is yes, then you need to stop.

72. When using the webcam be aware of what is in the camera's field of vision and remember to turn the camera off when it is not in use. Webcam sessions and photos can be easily captured, and users can continue to circulate those images online. In some cases people believed they were interacting with trusted friends but later found their images were distributed to others or posted on web sites.

73. Do not post identity-revealing or sexually provocative photos. Never post photos of others — even your friends — without permission from your friends' parents or guardians. Once such images are posted you relinquish control of them and can never get them back. Other people can use them for destructive purposes.

74. Immediately tell a trusted adult if you come across inappropriate material.

CYBER COMMUNITY - WIRELESS COMMUNICATION/TEXT MESSAGING

75. Never share your wireless number and personal or identifying information with anyone you don't know very well and trust.

76. Respect your friends' privacy by never sharing their number or information.

77. Never use your wireless device to take, send, or post pictures or video of your friends without permission from their parents or guardians. Taking or sharing embarrassing pictures of someone is a form of bullying and harassment. Once you post an image or video online you can't get it back.

78. Keep your passwords private. Never share them with anyone other than your parent or guardian.

79. Never give photos of yourself to anyone you don't know well. Never send obscene or sexually provocative pictures or messages.

80. Never respond to threatening or frightening voice messages, text messages, or photos. Report the incident to your parent/guardian and service provider.

81. Block unwanted calls and text messages. Never answer calls or read messages from people you don't know well and trust.

82. As cell phones and PDAs become more technologically advanced, attackers are finding new ways to target victims. By using text messaging or e-mail, an attacker can lure you to a site or convince you to install unwanted codes on your portable device.

83. Because wireless networks do not require a wire between a computer and the Internet connection, it is possible for attackers who are within range to hijack or intercept an unprotected connection. Change the default passwords and restrict access in order to minimize risks to your wireless network.

84. Keep in mind that text messages may be intercepted or used by others. Use appropriate language in your messages while being sure not to reveal personal or identifying information.

CYBER SECURITY - GAMING

85. Be aware of sexual predators and/or cyber bullies in gaming sites. Students need to talk with parents about what is acceptable.

Internet Safety Curriculum Resources

VDOE

Guidelines And Resources For Internet Safety In Schools, Office of Educational Technology
http://www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines.shtml

Guidelines And Resources for Internet Safety In Schools handbook

http://www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines-resources.pdf

Instructional Alignment, Office of Educational Technology, Media Services

http://www.doe.virginia.gov/VDOE/Technology?OET/llaa/materials.html

Sites for Educators, Students and Parents

http://www.isafe.org/ - i-Safe - Founded in 1998, i-SAFE America provides Internet safety information and knowledge to students, parents, and everyone in the community in a variety of ways.

http://www.netsmartz.org/ - NetSmartz - The NetSmartz Workshop is an educational resource for children of all ages, parents and teachers on how to stay safer on the Internet. The NetSmartz Workshop features age-appropriate, interactive games and activities that utilize the latest web technologies to entertain while they educate.

http://www.cyberbee.com/safety.html - Adventures of Cyberbee - Listing of several organized links on how to integrate Internet Safety into the classroom.

http://www.cybersmart.org/home/ - Cyber Smart - Comprehensive curriculum designed for teachers and parents is presented in an easy to use format. The content covers appropriate use of the Internet, property rights, ethics, and Website evaluation.

http://www.getnetwise.org/ - Get Net Wise - GetNetWise is a public service brought to you by Internet industry corporations and public interest organizations to help ensure that families have safe, constructive, and educational or entertaining online experiences. The GetNetWise coalition wants Internet users to be just "one click away" from the resources they need to make informed decisions about their family's use of the Internet. GetNetWise is a project of the Internet Education Foundation. In addition to the standard safety guide and parental tools, a much needed guide to how and where to report any trouble encountered on the Internet.

http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/index.html - Kidz Privacy - The Federal Trade Commission has created a Website for parents and kids with loads of tips on safety and privacy issues.

http://pbskids.org/license/ - "Rules of the Road" Internet Safety Quiz – A quiz that tests student's knowledge on Internet safety.

http://www.fbi.gov/publications/pguide/pguide.htm - Parents Guide to Internet Safety - A handbook published by the FBI.

http://home.disney.go.com/guestservices/safety - Surf Swell Island (Disney) – Offers parents the following tips to keep your child safe on the Internet.

http://www.newton.dep.anl.gov/teachers/compvir.htm - What Are Computer Viruses – Information about what computer viruses are, what they don't do, how they spread, how to prevent viruses, and examples of common viruses.

http://www.scholastic.com/toolkit/classport/play.htm - Safe Surf Quiz – Test online safety smarts. Students answer all questions correctly and get a certificate.

http://www.safekids.com/quiz/index.html - Safe Kids Quiz - The Online Safety Quiz gives students a chance to show that they know how to be a safe Internet surfer (Primary).

http://www.teachingideas.co.uk/welcome/searching/index.htm - Searching the Net – Step by step instructions on how students can search the internet safely.

http://www.learn4good.com/kids/internet_safety_tips.htm - Learn 4 Good – Internet Safety Tips for Parents on ways to protect their children.

http://hcpstraining.org/itrt/hcpsisafe/index.htm - Internet Safety - Contains information, activities, and videos on 6 levels. Also lists a parent guide.

http://www.gamequarium.com/internetsafety.html - Gamequarium - A listing of games and quizzes that review Internet Safety.

http://www.oag.state.va.us/KEY_ISSUES/FAMILY_INTERNET/index.html - Virginia Government – Resources, videos, suggestions and ideas on how parents can keep their families

safe on the Internet. http://www.staysafe.org/ - Stay Safe – Deals with online safety, security, cyberbullying, and cyberethics.

http://www.wiredkids.org/wiredkids_org.html - Wired Kids - Information about Cyberbullying, Flaming and Cyberstalking, for Kids, Tweens, Teens, Parents, Educators and Law Enforcement.

http://www.cyberbullying.org/ - Cyberbullying - Resources, Facts, What can be done, and more about cyberbullying.

http://www.cyberbullyhelp.com – Variety of educational resources to help prevent cyberbullying.

http://www.cybersmartcurriculum.org/home/ - CyberSmart – Lesson plans, activities, resources for K-12.

http://www.mcps.org/admin/Technology/TRTWebpage/isresource.htm - Montgomery County's resource page listing various activities, resources, powerpoints, videos, lessons, rules and pledges.

http://www.thebeehive.org/Templates/ComputerSupport/InternetNoRight.aspx?PageId=1.890.11426 – The Beehive – Information on how to protect your computer, computer lingo, online chatting guide, etc.

www.unitedstreaming.com – United Streaming – 45 videos related to Internet Safety including integration in the curriculum.

http://www.teachertube.com/search_result.php?search_id=Internet+Safety – Teacher Tube – Videos related to Internet Safety. Teaches will need to register prior to viewing.

http://www.mcps.org/admin/Technology/TRTWebpage/Internet_Safety_Curriculums/Elementary_3-5/ChecklistforInternetSafetyallgrades.doc

Internet Safety Curriculum-Compliance Checklist

Additional resources can be found in the *Guidelines and Resources for Internet Safety in Schools*, Virginia Department of Education, August 2007

References

Cannaday, B. (2007), Technology Acceptable Use Policy and Internet Implementation Rubrics, Retrieved on September 26, 2007, from http://www.doe.virginia.gov/VDOE/suptsmemos/2007/inf069.html

(2006), Legislation, Retrieved on September 26, 2007, from http://www.doe.virginia.gov/VDOE?Technology?OET/internet-safety-guidelinesresources.pdf, p.2

(2006), Virginia Acts VIRGINIA ACTS OF ASSEMBLY—2006 SESSION CHAPTER 52, Retrieved on September 26, 2007, from http://leg1.state.va.us/cgi/bin/leg504.exe?061+ful_HB58H1

07/11 Regulation 5.33

PERSONNEL

TECHNOLOGY: Computer and Telecommunications Guidelines and Responsibilities

A. Purpose

To provide guidelines and responsibilities for the use of the Information Technology and Telecommunications Systems provided by Manassas City Public Schools which are consistent with the division's educational objectives and security requirements. Access to networks both inside and outside of Manassas City Public Schools carries with it the responsibility for proper use of these resources.

B. Definitions

1. Computer System - Any computer owned by the Manassas City Public Schools that may or may not be connected to the WAN and Internet services.

2. Core System - A mission-critical application or system that is protected from general public access. (Mission Critical Application) - An operation that is immediately vital to the operation of an enterprise. If stopping the "system" stops the enterprise, then that system is mission critical.

3. Information System(s) - Includes, but is not limited to, hardware, software, terminals, printers, CD-ROM devices, tape drives and servers, mainframe and personal computers.

4. Internet Access - Includes all methodologies used to connect to individual computer networks around the world.

5. Internet Service Provider - The commercial vendor that Manassas City Public Schools uses on a contractual basis to provide the interface and or connectivity between the Manassas City Public Schools wide area network (WAN) and the Internet.

6. Internet Services - Includes access to external systems and information sources using the Internet; access to and hosting of World Wide Web (WWW) services and information; use of Internet tools such as FTP(File Transfer Protocol), gopher, Telnet, chat, E-mail, IRC (Internet Relay Chat), and Instant Messaging.

(continued)

07/11 Regulation 5.33

PERSONNEL

B. Definitions – (continued)

7. System-wide Information - Includes any information (data, statistics, publications, etc.) that pertains to the entire School Division or that involves more than one department.

8. Telecommunications System(s) – communication lines and devices - i.e. landline telephones, fax machines, and wireless communication devices

9. Users - Includes all staff, students, volunteers, parents or other individuals utilizing any portion of the Manassas City Public Schools Information Systems.

10. Webmaster - A person assigned by a school or department to maintain a set of web pages on the Manassas City Public Schools web server.

11. Web Page - A page of information located on a web server and accessible through the Internet. The page can contain a mixture of graphics and text and can include embedded references to other such pages.

12. Wide Area Network (WAN) - The network of all computers in Manassas City Public Schools that are connected to their building's local area network (LAN).

C. General Computer Use Guidelines

1. User Responsibilities

a. The use of computer systems for personal reasons unrelated to the mission of Manassas City Public Schools or for private gain is prohibited. Using the computer for commercial, religious or political purposes is prohibited.

b. All access to Manassas City Public Schools computer systems shall be approved by the appropriate program manager.

c. No user shall vandalize the computer system and data, including destroying data by creating or spreading viruses or by other means.

d. Users are prohibited from using the computer system while access privileges are suspended or revoked.

(continued)

07/11 Regulation 5.33

PERSONNEL

User Responsibilities - (continued)

e. Computers owned by the private individual may be used in the Manassas City Public Schools. However, software purchased by the School Division may not be used without written authorization from the Supervisor of Administrative and/or Instructional Technology or designee.

f. Privately owned computers may not be connected to the Manassas City Public Schools Wide Area Network without written authorization from the Supervisor of Administrative Technology and/or Instructional Technology or designee.

g. Manassas City Public Schools personnel shall not service any privately owned personal computers. Any damage caused by use in the Manassas City Public Schools is the responsibility of the owner.

h. No privately owned computer may contain any internal pieces of equipment (memory, disk drives, expansion boards, etc.) that has been purchased by or for the Manassas City Public Schools.

i. Users must agree to the MCPS Computer and Telecommunications Systems user guidelines and provide a signed copy

2. Network Access

a. Users shall not reveal their passwords to anyone without prior approval.

b. Users are prohibited from using or sharing passwords and IDs other than those specifically assigned to them.

c. Users are prohibited from wastefully using resources, such as file space

d. Access to Manassas City Public Schools Core Systems is prohibited unless otherwise pre-approved by Supervisor of Administrative Technology or designee

e. Circumventing security measures on school or remote computers or networks.

(continued)

PERSONNEL

3. Internet Access and Email Access

a. All users are prohibited from accessing portions of the Internet that do not promote the educational mission or administrative function of the Manassas City Public Schools during regular working hours.

b. Outbound access to the Internet shall be in accordance with applicable Manassas City Public Schools rules and regulations. Monitoring and management of acceptable use is the responsibility of the program-manager.

c. Inbound access to Manassas City Public Schools systems and services from the Internet shall be restricted to the Manassas City Public Schools dial in server unless otherwise authorized by the Supervisor of Instructional Technology or designee. This prohibition includes Internet services such as FTP, Telnet, time, gopher, ping, Netbus, finger, etc.

d. Copyrighted software shall not be downloaded from the Internet or further transmitted in any form without compliance with all terms of a pre-authorized licensing agreement. Manassas City Public Schools will not tolerate infringement or violation of United States or international copyright laws or restrictions.

e. The City of Manassas Public Schools is not responsible for any information that may be lost, damaged or unavailable when using the computer systems or for any information retrieved via the Internet.

f. The City of Manassas Public Schools will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

g. The City of Manassas Public School's electronic mail system is owned and controlled by the School Division. The School Division may provide electronic mail to aid students and staff in fulfilling their duties as an education tool. Electronic mail is not private and may be monitored and accessed by the School Division. Unauthorized access to an electronic mail account by any student or employee is prohibited. Users shall be held personally responsible for the content of any electronic message sent from their account. Downloading any file attached to an electronic message is prohibited unless the user is certain of that message's authenticity and the nature of the file.

PERSONNEL

h. The City of Manassas Public Schools makes no warranties of the computer system it provides. The School Board shall not be responsible for any damages to the user from use of the computer system, including loss of data, non-delivery or missed delivery of information, or service interruptions. The School Division denies any responsibility for the accuracy or quality of information obtained through the computer system. The user agrees to indemnify the School Board for any losses, costs or damages incurred by the School Board relating to or arising out of any violation of these procedures.

D. Webpage

1. The City of Manassas Public Schools has created a web site on the Internet with accompanying web pages for each school. There are several important purposes for this website. The website may be used as a public relations tool highlighting school and school division achievements, student accomplishments and, at the same time, to build support for the Technology Initiative. The website can be used to increase awareness about activities at each school and describe resources which are available to parents and students. By far one of the most important benefits of creating a website is to give students in each of our schools an opportunity to establish and maintain the site under the supervision of an adult.

2. Listed below are important school/Division guidelines for establishing a webpage on the Internet. It is important that all schools follow these guidelines.

   a. Names and/or pictures of students may be posted with parental permission.

   b. Text and/or graphics may not be posted if it:

      1) Discriminates on the basis of sex, race, age, color, religion, disabilities, or national origin, or harasses an employee, student, or other person.

      2) Portrays nudity or deals with human sexuality.

      3) May cause disruption of school activities (such as by encouraging a riot or destruction of property, being damaging to morale, or being harshly critical of policy).

(continued)

PERSONNEL

E. Webpage – (continued)

4) Is not approved by the school administrator or designee, or a central office supervisor.

5) Is created by another and used without his or her consent.

6) Represents personal views as those of the School Board or administration.

c. Links to outside web pages are subject to the same substantive guidelines as E 2.b above.

d. If any Manassas City Public Schools employee becomes aware that a web page contains questionable material, the employee is expected to notify the immediate responsible administrator, teacher, or supervisor who will determine if any applicable policies, guidelines, rules or regulations have been violated and take the appropriate action.

e. School home pages shall contain the following minimum items:

1) School name, address and telephone numbers

2) School Profile

3) Links to all important school related information

4) Administrators' names and E-mail addresses (secure information)

5) Welcome message from the principal

f. School home pages shall be updated monthly during the school year

g. Webpage Publishing:

1) The establishment of web pages on the Internet must have an educational purpose that is related to a Manassas City Public School assignment, project, job, or function.

(continued)

PERSONNEL

E. Webpage – (continued)

2) All system-wide information to be published on the Internet must be reviewed and approved by the Deputy Superintendent or designee prior to being uploaded to the Manassas City Public Schools web server.

3) Copyrighted material shall not be placed upon any part of a webpage without prior permission from the copyright owner.

4) Information may not be posted on the Internet if it: violates the privacy of others, jeopardizes the health and safety of students or employees, is obscene or libelous, causes disruption of school activities, plagiarizes the work of others, is a commercial advertisement, or is not approved by the principal or program manager.

5) All web pages must include the name of the responsible Manassas City Public Schools official, the name of the webmaster, and the date that the page was last updated.

F. Responsibilities: If any Manassas City Public Schools employee becomes aware that a webpage contains questionable material, the employee is expected to notify the responsible administrator or supervisor who will determine if any applicable policies, guidelines, rules or regulations have been violated and take the appropriate action.

G. Consequences: It is the policy of the City of Manassas Public Schools to protect computing resources under its management from unauthorized access, use, modification, copying and destruction. The City of Manassas Public Schools will take appropriate disciplinary action against any person who breeches this policy. Such action may include dismissal.

PERSONNEL

H. Measures Taken to Ensure Internet Safety

1. As stated in this regulation, penalties or disciplinary actions such as student suspensions, teacher dismissal, or revocation of use privilege may result if a violation occurs. The action depends on the severity of the violation.

2. City of Manassas Public Schools reserves the right to monitor Internet and Email use, and web postings by teachers, students, administrators and support staff.

3. All City of Manassas Public Schools employees and students should recognize and use their responsibility to refrain from inappropriate use of the Internet or Email.

4. City of Manassas Public Schools uses internet filtering software. As a server-based solution, it allows Manassas City Public Schools to transparently monitor, manage, and report traffic flowing from internal networks to the internet. This software also aids the division in the conservation of precious network bandwidth resources, the reduction of legal liability, the boosting of employee productivity, and the enforcement of the existing Manassas City Public Schools policy pertaining to internet access.

5. City of Manassas Public Schools uses desktop security software in order to ensure that all computers are free from inappropriate tampering.

I. Telecommunications Use – Guidelines

1. The City of Manassas Public Schools provides telecommunications services and devices (communication lines, fax machines, wireless devices, etc.) are provided for teaching, research and administrative duties on behalf of the school system. Improper use of the services can be considered misappropriation of school division funds and could jeopardize the school division's non-profit status.

2. The City of Manassas Public Schools will not be responsible for any unauthorized charges or fees. Accepting collect calls is prohibited.

3. Personal long distance calls are not to be made from school division telephones. Any such call must be charged to the caller's home telephone, personal credit or calling card or to another non-school source.

4. User shall refrain from the making and the receiving of *excessive personal* calls

5. Users are prohibited from using division telecommunication resources for commercial, religious, political or financial gain or related to outside employment or business ownership.

6. Users are prohibited from damaging or destroying telecommunication equipment or deliberately degrading the system performance, including deliberate infection of phones,

computers or servers with viruses

7. Users are prohibited from disclosing a voicemail password to another employee or to a student, or attempts to disclose or discover another employee's voicemail password.

8. Users are prohibited from using a telecommunication device and or any attached equipment to obtain and or distribute illegally duplicated and distributed digital music, video and or software from copyrighted sources if your telecommunication device is web enabled.

9. Users are prohibited from using the telecommunication equipment for illegal, inappropriate, subversive or obscene purposes or activities.

10. User should understand that detailed monthly telephone records are monitored and are considered public records and subject to disclosure.

Approved by Superintendent: November 1, 1999

Amended by Superintendent: October 9, 2001

Amended by Superintendent: October 28, 2005

Amended by Superintendent: June 7, 2007
Amended by Superintendent: July 19, 2011

10/05 Regulation 7-60

STUDENTS

TECHNOLOGY: GUIDELINES AND RESPONSIBILITIES

A. Generally: To provide guidelines and responsibilities for the use of the Information Technology provided by the Manassas City Public Schools (Manassas City Public Schools) which are consistent with Manassas City Public Schools educational objectives and security requirements. This regulation covers all Information Technology and services provided by Manassas City Public Schools and used by Manassas City Public Schools students, staff and administrators. Manassas City Public Schools provides computer equipment, computer services and networks including computer Internet access for **educational and administrative purposes only**. All use of the Manassas City Public School's computer system must be (1) in support of education and/or research, or (2) for legitimate school business. Access to networks both inside and outside of Manassas City Public Schools carries with it the responsibility for proper use of these resources.

B. Definitions

1. Computer System - Any computer owned by the Manassas City Public Schools that may or may not be connected to the WAN and Internet services.
2. Core System - A mission-critical application or system that is protected from general public access. (Mission Critical Application) - An operation that is immediately vital to the operation of an enterprise. If stopping the "system" stops the enterprise, then that system is mission critical.
3. Information System(s) - Includes, but is not limited to, hardware, software, communication lines and devices, terminals, printers, CD-ROM devices, tape drives and servers, mainframe and personal computers.
4. Internet Access - Includes all methodologies used to connect to individual computer networks around the world.
5. Internet Service Provider - The commercial vendor that Manassas City Public Schools uses on a contractual basis to provide the interface and or connectivity between the Manassas City Public Schools wide area network (WAN) and the Internet.
6. Internet Services - Includes access to external systems and information sources using the Internet; access to and hosting of World Wide Web (WWW) services and information; use of Internet tools such as FTP(File Transfer Protocol), gopher, Telnet, chat, E-mail, IRC (Internet Relay Chat), and Instant Messaging.
7. System-wide Information - Includes any information (data, statistics, publications, etc.) that pertains to the entire School Division or that involves more than one department.
8. Users - Includes all staff, students, volunteers, parents or other individuals utilizing any portion of the Manassas City Public Schools Information Systems.
9. Webmaster - A person assigned by a school or department to maintain a set of web pages on the Manassas City Public Schools web server.
10. Web Page - A page of information located on a web server and accessible through the Internet. The page can contain a mixture of graphics and text and can include embedded references to other such pages.
11. Wide Area Network (WAN) - The network of all computers in Manassas City Public Schools that are connected to their building's local area network (LAN).

C. Student Guidelines

1. Computer Use

a. Computer users will:

1) Employ appropriate language;

2) Avoid offensive or inflammatory speech;

3) Avoid copyright infringement;

4) Respect the rights to privacy of other users;

5) Not participate in illegal activities;

6) Respect the integrity of computing systems including hardware and software;

7) Conduct themselves responsibly when participating in "virtual electronic field trips". Inform teachers or administrators of any inappropriate conduct that restricts or inhibits any other user from accessing computer/Internet resources.

b. All access to Manassas City Public Schools systems shall be approved by the appropriate principal/program manager.

c. The use of computer systems for personal reasons unrelated to the mission of Manassas City Public Schools or for private gain is prohibited. Using the computer for commercial or private advertising is prohibited.

d. Users are prohibited from using the computer system while access privileges are suspended or revoked.

e. Computers owned by the private individual may be used in the Manassas City Public Schools. However, software purchased by the School Division may not be used without written authorization from the Supervisor of Instructional Technology or designee.

f. Privately owned computers may not be connected to the Manassas City Public Schools Wide Area Network without written authorization from the Supervisor of Instructional Technology.

g. Manassas City Public Schools personnel shall not service any privately owned personal computers. Any damage caused by use in the Manassas City Public Schools is the responsibility of the owner.

h. No privately owned computer may contain any internal pieces of equipment (memory, disk drives, expansion boards, etc.) that has been purchased by or for the Manassas City Public Schools.

i. No user shall vandalize the computer system, including destroying data by creating or spreading viruses or by other means.

2. Network Access

a. Access to Manassas City Public Schools Core Systems is prohibited. Any attempt at acquiring information from these systems will be dealt with suspension of computer use and/or any disciplinary actions listed in the Manassas City Public Schools Student Conduct Code.
b. Users shall not reveal their passwords to anyone without prior approval by the principal or teacher.
c. Users are forbidden from using passwords and IDs other than those specifically assigned to them.
d. Copyrighted software shall not be downloaded from network resources or further transmitted in any form without compliance with all terms of a pre-authorized licensing agreement. Manassas City Public Schools will not tolerate infringement or violation of United States or international copyright laws or restrictions.

3. Internet and Email Access

i. All users are prohibited from accessing portions of the Internet that do not promote the educational/instructional mission of the Manassas City Public Schools.
j. Outbound access to the Internet shall be in accordance with applicable Manassas City Public Schools rules and regulations. Monitoring and management of acceptable use is the responsibility of the principal or teacher.
k. Inbound access to Manassas City Public Schools systems and services from the Internet shall be restricted to the Manassas City Public Schools dial in server unless otherwise authorized by the Supervisor of Instructional Technology or designee. This prohibition includes Internet services such as FTP, Telnet, time, gopher, ping, Netbus, finger, etc.
l. Copyrighted software shall not be downloaded from the Internet or further transmitted in any form without compliance with all terms of a pre-authorized licensing agreement. Manassas City Public Schools will not tolerate infringement or violation of United States or international copyright laws or restrictions.
m. The City of Manassas Public School's electronic mail system is owned and controlled by the School Division. The School Division may provide electronic mail to aid students and staff in fulfilling their duties and as an education tool. Electronic mail is not private and may be monitored and accessed by the School Division. Unauthorized access to an electronic mail account by any student is prohibited. Users shall be held personally liable for the content of any electronic message they create. Downloading any file attached to an electronic message is prohibited unless the user is certain of that message's authenticity and the nature of the file.
n. Users will never give out identifying information (name, home address, telephone number, pictures, etc. unless authorized by Manassas City Public Schools and parents;
o. Users will not arrange face-to-face meetings with others through the Internet;
p. Users will not create, peruse, or respond to messages or bulletin items that are sexually suggestive, obscene, belligerent, threatening, or that are otherwise inappropriate in an educational setting.
q. Users will inform teachers and/or administrators of any threatening or unwelcome communications;

r. Users will always adhere to the standards set by the attending professional educators and by their parents/guardians.
s. The City of Manassas Public Schools assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including telephone or long-distance charges.
t. The School Board shall not be responsible for any damages to the user from use of the computer system, including loss of data, non-delivery or missed delivery of information, or service interruptions. The School Division denies any responsibility for the accuracy or quality of information obtained through the computer system. The user agrees to indemnify the School Board for any losses, costs or damages incurred by the School Board relating to or arising out of any violation of these procedures.

4. Web Page Publishing

a. The establishment of web pages on the Internet by Manassas City Public Schools staff and students that are stored and served by Manassas City Public Schools equipment must have an educational purpose that is related to a Manassas City Public School assignment, project, job or function.
b. All system-wide information to be published on the Internet must be reviewed and approved by the Deputy Superintendent or designee prior to being uploaded to the Manassas City Public Schools web server.
c. Names and/or pictures of students may be posted with parental permission
d. Information may not be posted, if it:

1) Discriminates on the basis of sex, race, age, color, religion, disabilities, or national origin
2) Violates the privacy of others
3) Jeopardizes the health or safety of students
4) Portrays nudity or deals with human sexuality
5) Is libelous
6) Causes disruption of school activities (i.e. encouraging a riot, destruction of property, etc.
7) Violates copyright
8) Plagiarizes the work of others
9) Is not approved by the school administrator or designee, or a central office supervisor

e. Links to outside web pages are subject to the same substantive guidelines as "d" above.

f. Copyrighted material shall not be placed upon any part of a web page without prior permission from the copyright owner.

g. If any Manassas City Public Schools employee becomes aware that a web page contains questionable material, the employee is expected to notify the immediate responsible administrator, teacher, or supervisor who will determine if any applicable policies, guidelines, rules or regulations have been violated and take

the appropriate action.

h. School home pages shall contain the following minimum items:

1) School name, address and telephone numbers
2) School Profile
3) Links to all important school related information
4) Administrators' names and E-mail addresses (secure information)
5) Welcome message from the Principal

i. School home pages shall be updated monthly during the school year

D. Measures Taken to Ensure Internet Safety

1. As stated in this regulation, penalties or disciplinary actions such as student suspensions, teacher dismissal, or revocation of use privilege may result if a violation occurs. The action depends on the severity of the violation.
2. City of Manassas Public Schools reserves the right to monitor Internet and Email use, and web postings by teachers, students, administrators and support staff.
3. All City of Manassas Public Schools employees and students should recognize and use their responsibility to refrain from inappropriate use of the Internet or Email.
4. City of Manassas Public Schools uses internet filtering software. As a server-based solution, it allows Manassas City Public Schools to transparently monitor, manage, and report traffic flowing from internal networks to the internet. This software also aids the division in the conservation of precious network bandwidth resources, the reduction of legal liability, the boosting of employee productivity, and the enforcement of the existing Manassas City Public Schools policy pertaining to Internet access.
5. City of Manassas Public Schools uses desktop security software in order to ensure that all computers are free from inappropriate tampering.

Approved by Superintendent: November 1, 1999

Amended by Superintendent: October 9, 2001

Amended by Superintendent: October 28, 2005

Amended by Superintendent: June 7, 2007

06/06 Regulation 7-60

STUDENTS

ACCEPTABLE USE OF INFORMATION TECHNOLOGY

The Division Superintendent shall establish administrative procedures, for the School Board's approval, containing the appropriate uses, ethics and protocol for the division's computer system and facilities as they relate to the areas listed below:

A. City of Manassas Public Schools provides computer equipment, computer services and network access to students for educational purposes only. These services are provided to improve learning and teaching through research and expanded use of materials and resources.

B. Educational purposes are defined as those purposes directly related to a City of Manassas Public School assignment, project, task or any other function for which the student is responsible.

C. Access to networks both inside and outside of Manassas City Schools carries with it the responsibility for proper use of those resources and Manassas City School's computing facilities. Use of the computer system is a privilege, not a right.

The City of Manassas Public Schools recognizes the fact that most computer users are responsible, thoughtful users. However, the actions of irresponsible users can disrupt and interfere with the rights of all users. The Board also recognizes the rights of administrators and teachers to develop consequences for the inappropriate use of school division technology.

Adopted by School Board: June 27, 2006