VIRGINIA DEPARTMENT OF EDUCATION

REPORT

ACCEPTABLE INTERNET USE POLICIES AND INTERNET SAFETY PROGRAMS FOR PUBLIC AND PRIVATE SCHOOLS

PRESENTED TO THE

GOVERNOR OF VIRGINIA AND THE VIRGINIA GENERAL ASSEMBLY

December 2008

COMMONWEALTH of VIRGINIA

Patricia I. Wright, Ed.D.
Superintendent of Public Instruction

DEPARTMENT OF EDUCATION
P.O. BOX 2120
Richmond, Virginia 23218-2120

Office: (804) 225-2023
Fax: (804) 371-2099

December 17, 2008

The Honorable Timothy M. Kaine
Governor of Virginia
Patrick Henry Building, 3rd Floor
1111 East Broad Street
Richmond, Virginia 23219

The Honorable Kathy J. Byron
Chair, House Science & Technology Committee
523 Leesville Road
Lynchburg, Virginia 24502

The Honorable R. Edward Houck
Chairman, Education & Health Committee
Post Office Box 7
Spotsylvania, Virginia 22553

The Honorable Robert Tata
Chairman, House Education Committee
4536 Gleneagle Drive
Virginia Beach, Virginia 23462

Dear Governor Kaine, Senator Houck, and Delegates Byron and Tata:

Pursuant to Section 22.1–70.2 of the *Code of Virginia*, I am pleased to submit the following biennial report: *Acceptable Internet Use Policies and Internet Safety Programs for Public and Private Schools*.

If you have any questions or require additional information, please contact me at (804) 225-2023.

Sincerely,

Patricia I. Wright

PIW/slm
Attachment

CONTENTS

EXECUTIVE SUMMARY

The Internet has become even more ubiquitous since the Department of Education's last report to the General Assembly in 2006. Teachers and students have found new educational uses for the Internet and other related technologies, such as wireless handheld devices. Online classes are increasingly common methods for student learning. As a result, students have a greater choice in how, when, and where they learn. A challenge, though, is that the pervasiveness of the Internet and the inclusion of new information and communication technologies have generated new issues related to student safety.

As in the past, the General Assembly has led the way for the nation. In 2006, House Bill 58, introduced by Delegate William H. Fralin, Jr., directed that school divisions' acceptable use policies (AUP) "include a component on Internet safety for students that is integrated in a division's instructional program." With the passage of the Broadband Data Improvement Act of 2008, the nation's schools will now be required to follow Virginia's lead. Signed by President Bush on October 10, the Broadband Data Improvement Act requires schools receiving E-Rate funds to educate minors regarding Internet safety.

This document constitutes the Superintendent of Public Instruction's report on school division AUP for the reporting period December 2, 2006, to December 1, 2008. The report also provides examples of how the Department of Education has assisted school divisions in implementing House Bill 58. It summarizes the status of school divisions regarding compliance with this same bill.

In sum, all Virginia school divisions have complied with § 22.1-70.2 by submitting their AUP and summaries of their Internet safety programs to the Department of Education by September 1, 2008; the Department has reviewed all the submittals. About half the divisions still need improvement to achieve "Meets Expectations" in each area; most commonly, these areas are community outreach and good program implementation practice. Only three divisions have not reviewed their filtering and other Internet security software recently to ensure it is up-to-date. All divisions have complete and recently revised AUP.

Over this two-year period, the Department researched and developed various resource documents to help divisions develop and implement their AUP and Internet safety programs. The Department supplied compliance review rubrics to help divisions review their AUP and Internet safety programs; the Department used these same rubrics to analyze the submitted materials. The Department, in collaboration with Pokémon USA, launched a pilot program using Web-based interactive lessons about Internet safety. These high-interest lessons were based, in part, on Virginia's *Guidelines and Resources for Internet Safety in Schools*. Research indicates the lessons were successful in changing student behavior.

During the next two-year period, the Department will continue providing support to divisions in implementing Internet safety programs, offering up-to-date information related to Internet safety issues, and enforcing compliance and reporting procedures.

INTRODUCTION

The Virginia General Assembly consistently has enacted legislation to promote the Internet's instructional benefits while protecting students from its risks.

House Bill 1043, enacted in 1999, amended the *Code of Virginia* by adding § 22.1-70.2 to Chapter 6 of Title 22.1, which details the duties of the Superintendent of Public Instruction regarding acceptable Internet use policies. The act required school divisions to develop acceptable use policies (AUP) that outline Internet guidelines for students and teachers, protect children's rights, and convey responsibilities each student must assume while using the Internet as an educational tool. Moreover, these policies posit expectations, establish rights, and draw lines of responsibility for the entire school community.

In response to this legislation, all 132 school divisions submitted to the Department of Education AUP that (1) prohibit students and employees from using the Internet to send, receive, view, or download illegal material; (2) prevent students under age 18 from accessing material considered harmful to juveniles; and (3) establish appropriate measures for persons who violate the policy. Most of these AUP include disclaimer statements and signature forms for students, teachers, and parents to confirm they have read the policy and will abide by its terms. Section 22.1-70.2 also directed the Superintendent of Public Instruction to submit a report on or before December 1, 2000, and biennially thereafter, that summarizes the divisions' AUP filed with the Superintendent. In 2001, new state and federal laws authorized the installation of filtering software to prevent students from accessing potentially harmful material. As a result, each division submitted a letter of assurance stating that all schools were in compliance with the installation of filtering technologies.

In 2006, the legislature passed House Bill 58, introduced by Delegate William H. Fralin, Jr., mandating that divisions' AUP "include a component on Internet safety for students that is integrated in a division's instructional program" (see "Authority for the Report"). The new legislation required the Superintendent of Public Instruction to issue Internet safety guidelines to divisions. Subsequently, the Department of Education released *Guidelines and Resources for Internet Safety in Schools* in October 2006; these were revised in fall 2007 to reflect new laws and research findings.

The Virginia Department of Education has researched and developed various resource documents to help divisions develop and implement their AUP and Internet safety programs. The Department also has worked with other organizations throughout the state to ensure that all stakeholders are aware of the requirements of and good practices related to teaching Internet safety.

During the 2007-08 school year, the Department of Education, in collaboration with Pokémon USA, launched a pilot program using Web-based interactive lessons about Internet safety. These high-interest lessons were based, in part, on Virginia's *Guidelines*

and Resources for Internet Safety in Schools. Research indicates the lessons were successful in changing student behavior. About half of Virginia's fourth graders will have access to these lessons during the 2008-09 school year; schools were selected for participation based on levels of bullying-related incidents reported in the Discipline, Crime, & Violence: Annual Reports.

The Department developed and distributed rubrics to divisions that detail the various requirements of § 22.1-70.2 along with best practices in program implementation. These rubrics were used to review the AUP and Internet safety program of each division. The rubrics are included as Appendix C, and the summary of the review results is detailed in Appendix D.

AUTHORITY FOR THE REPORT

In 2006, the legislature passed House Bill 58, introduced by Delegate William H. Fralin, Jr., mandating that school divisions' AUP "include a component on Internet safety for students that is integrated in a division's instructional program." House Bill 58 amended § 22.1-70.2 of the *Code of Virginia* as follows:

§ **22.1-70.2**. Acceptable Internet use policies for public and private schools.

A. Every two years, each division superintendent shall file with the Superintendent of Public Instruction an acceptable use policy, approved by the local school board, for the Internet. At a minimum, the policy shall contain provisions that (i) are designed to prohibit use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet; (ii) seek to prevent access by students to material that the school division deems to be harmful to juveniles as defined in § **18.2-390**; (iii) select a technology for the division's computers having Internet access to filter or block Internet access through such computers to child pornography as set out in § **18.2-374.1:1** and obscenity as defined in § **18.2-372**; (iv) establish appropriate measures to be taken against persons who violate the policy; and (v) include a component on Internet safety for students that is integrated in a division's instructional program. The 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.

B. The superintendent shall take such steps as he deems appropriate to implement and enforce the division's policy.

C. On or before December 1, 2000, and biennially thereafter, the Superintendent of Public Instruction shall submit a report to the Chairmen of the House Committee on Education, the House Committee on Science and Technology, and the Senate Committee on Education and Health which summarizes the acceptable use policies filed with the Superintendent pursuant to this section and the status thereof.

D. In addition to the foregoing requirements regarding public school Internet use policies, the principal or other chief administrator of any private school that satisfies the compulsory school attendance law pursuant to § **22.1-254** and accepts federal funds for Internet access shall select a technology for its computers having Internet access to filter or block Internet access through such computers to child pornography as set out in § **18.2-374.1:1** and obscenity as defined in § **18.2-372**.

E. The Superintendent of Public Instruction shall issue guidelines to school divisions regarding instructional programs related to Internet safety.

(1999, c. 64; 2001, c. 269; 2006, cc. 52, 474.)

ACTIVITIES DURING THE REPORTING PERIOD

During this reporting period, major activities focused on helping school divisions create strong Internet safety programs and reviewing AUP and Internet safety programs for compliance. To that end, the Department of Education completed these specific tasks:

Provided Support to School Divisions Creating Internet Safety Programs

- Developed *Ideas for Integrating Internet Safety into the Curriculum*, a document that could help teachers find ways to incorporate Internet safety topics in their regular curricula
- Worked with library media specialists from around the state to update their organization's *Linking Libraries* document—which relates library goals to Virginia standards—to include tips on incorporating Internet safety elements
- Presented information related to Internet safety programs at statewide and regional conferences and meetings
- Provided technical assistance to divisions that wished to have their programs reviewed
- Developed a pilot project using online interactive lessons on Internet safety topics targeting upper elementary students; topics include online safety, cyberbullying, distinguishing fact from opinion, and understanding forms of media; research shows this pilot had a positive effect on the retention of Internet safety behavior among participating students (see Appendix E for research results)

Offered Up-to-Date Information Related to Internet Safety Issues

- Updated *Guidelines and Resources for Internet Safety in Schools* to reflect new research and information
- Added new resources to *Related Resources for Internet Safety in Schools* at least twice each year
- Provided one-page summary of *Recent Studies, Surveys and Reports Regarding Internet Safety*
- Conducted and published an interview with Dr. Zheng Yan, an expert researcher on children and the Internet, with a focus on how his research can help divisions develop effective Internet safety programs
- Developed an *Information Brief*, in conjunction with the Virginia Attorney General's office, to help schools develop locally appropriate policies on cyberbullying (see Appendix B for the Superintendent's Memo announcing this brief)

Enforced Compliance and Reporting Procedures

- In January 2007, the Department released rubrics to determine division compliance with the guidelines for Internet safety, which incorporated model program implementation principles.

- Each division revised its AUP to include an Internet safety component in schools in 2006-07.
- By June 1, 2007, each division developed an Internet safety policy and program aligned with the state guidelines and incorporated into the AUP.
- During 2007-08, each division reviewed the progress and effectiveness of its Internet safety policy and the implementation of its Internet safety program.
- By September 1, 2008, each division submitted to the Department a copy of its revised AUP, a copy of its Internet safety policy, and a statement certifying that the policy and Internet safety program had been reviewed by a representative group of key stakeholders (see Appendix A for the Superintendent's Memo reminding divisions of this responsibility).
- During fall 2008, the Department reviewed division policies and provided detailed feedback to each division regarding their AUP and Internet safety programs.

SUMMARY OF RESULTS FROM REVIEW OF ACCEPTABLE USE POLICIES AND INTERNET SAFETY PROGRAMS

All divisions have complete and recently revised AUP. Within the division implementation rubrics parameters, in general, all divisions are meeting expectations or making progress toward expectations. Community outreach is one area where divisions are struggling more than others, with about half only making progress rather than meeting expectations. Parents are generally the only identified audience for outreach activities, though some exceptional divisions have created model community-based outreach programs. The Department will provide additional technical assistance to divisions that did not meet expectations.

A number of divisions have had some difficulty developing support systems to keep their Internet safety programs up-to-date and to increase the effectiveness of their programs. The Department can also support this area with technical assistance and by encouraging divisions with good program support structures to share information with those that do not.

Only three divisions have not reviewed their filtering and other Internet security software recently to ensure it is up-to-date. It is clear that divisions are well prepared to address the hardware/software interventions that help students stay safe while at school.

Several divisions have developed exemplary programs. These programs have been based both on best practices for implementing new programs and good Internet safety materials. They have been planned, implemented, evaluated, and revised using input from the community, involving all stakeholders. One of the best models is from Pittsylvania County in southern Virginia. Harrisonburg City, Stafford County, Caroline County, and Roanoke City also have created exemplary programs. Most of these divisions have strong Internet safety Web pages to support teachers, parents, students, and the community at large.

Appendix A

Superintendent's Memo No. 172
August 1, 2008

COMMONWEALTH OF VIRGINIA
DEPARTMENT OF EDUCATION
P.O. BOX 2120
RICHMOND, VIRGINIA 23218-2120

SUPTS. MEMO NO. 172
August 1, 2008

INFORMATIONAL

TO: Division Superintendents

FROM: Billy K. Cannaday, Jr.
Superintendent of Public Instruction

SUBJECT: Division Acceptable Use Policy Reporting Requirements

Legislation approved by the 2006 General Assembly and signed by Governor Kaine requires the addition of a student Internet safety component to division acceptable use policies (AUP). Original Superintendent's Memo No. 210 dated October 6, 2006, concerning *Code* § 22.1-70.2. Acceptable Internet use policies for public and private schools can be found at **http://www.doe.virginia.gov/VDOE/suptsmemos/2006/inf210.html**.

To comply with this legislation, each division must submit three documents to the Department's Office of Educational Technology (OET) by September 1, 2008:

- a copy of your updated acceptable use policy (AUP) which includes the Internet safety component
- a brief outline of the Internet safety program that is being used to integrate Internet safety into the curriculum
- a statement from the Division Superintendent that the acceptable use policy (including the Internet safety component) and the Internet safety program have been reviewed and adjusted during the 2007-2008 school year by those specified in the acceptable use policy as having this responsibility, and that the most recent policy has been approved by the local school board

It is preferable that all of these documents be submitted electronically. If you have submitted your updated technology plan (to Mark Saunders in OET) which includes your most recent AUP, you do not need to submit the first document. However, the other two items must be submitted to Jean Weller at **jean.weller@doe.virginia.gov** by September 1.

Please refer to the *Division Implementation Rubrics for Acceptable Use Policy and Internet Safety Program*

(**http://www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-rubrics.pdf**) for specific information about how the policy and program will be evaluated by the Virginia Department of Education in preparation for our biannual report to the General Assembly.

Questions about the acceptable use policy should be directed to Jean Weller, educational technology specialist, at (804) 225-2825 or e-mail at **jean.weller@doe.virginia.gov**.

BKCJr/jw/

Appendix B

Superintendent's Memo No. 239
September 26, 2008

COMMONWEALTH OF VIRGINIA
DEPARTMENT OF EDUCATION
P.O. BOX 2120
RICHMOND, VIRGINIA 23218-2120

SUPTS. MEMO NO. 239
September 26, 2008

INFORMATIONAL

TO: Division Superintendents

FROM: Billy K. Cannaday, Jr.
Superintendent of Public Instruction

SUBJECT: Cyberbullying and School Policy Information Brief

Cyberbullying, using communication technologies for bullying purposes, is a widespread and complex issue that must be addressed by schools at the policy level. To help school divisions develop effective policies regarding cyberbullying, the Virginia Department of Education's Office of Educational Technology and the Office of the Attorney General of Virginia have prepared an information brief. It may be found at **http://www.doe.virginia.gov/VDOE/Technology/OET/info_brief_cyberbullying.pdf**.

The information brief includes concrete examples of cyberbullying, a summary of legal issues involved, and expert recommendations for school policies and procedures. Also included is a model policy developed by the Virginia Attorney General's office, should divisions choose to create a separate cyberbullying policy.

Because cyberbullying crosses boundaries of school authority, it will most effectively be addressed when Internet safety, character education, and safe school committees work together. References, additional resources, and relevant articles are provided in the brief for use by these groups.

Questions may be directed to Jean Weller, educational technology specialist, at (804) 225-2825 or e-mail at **jean.weller@doe.virginia.gov**.

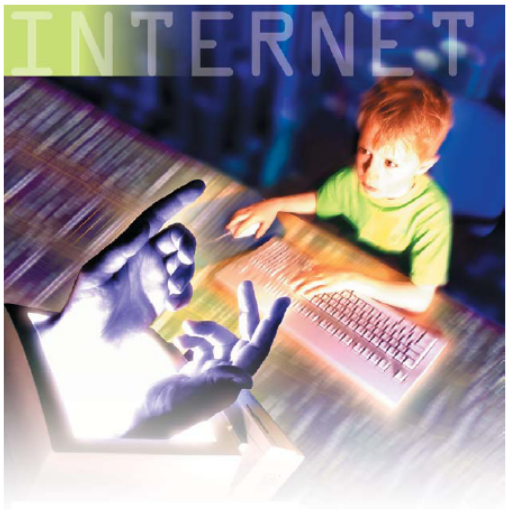
BKCJr/jw/fc

Appendix C

Division Implementation Rubrics

VIRGINIA DEPARTMENT OF EDUCATION
DIVISION OF
TECHNOLOGY & HUMAN RESOURCES
OFFICE OF EDUCATIONAL TECHNOLOGY

DIVISION IMPLEMENTATION RUBRICS FOR ACCEPTABLE USE POLICY AND INTERNET SAFETY PROGRAM



In 1999, the Virginia General Assembly passed legislation that added §22.1-70.2 to the *Code of Virginia*. Title §22.1-70.2 requires every division superintendent to file biennially with the Superintendent of Public Instruction an acceptable use policy, approved by the local school board, for the international network of computer systems commonly known as the Internet. The *Code* was amended in July 2001 to require each school division to select a filtering technology for all Internet-accessible computers. In 2006, the *Code* was amended again to require the integration of an Internet safety component into each division's instructional program.

The Superintendent of Public Instruction must submit a biennial report to the Virginia legislature stating that all school divisions are in compliance with this legislation. To that end, each school division is required to file an updated acceptable use policy to the Department of Education biennially. The deadline for the next submission is September 1, 2008, by which time each acceptable use policy must include an Internet safety component. The benchmarks for developing and implementing the component are as follows:

- During school year 2006-2007, each division will develop an Internet safety policy, which must be aligned with the state guidelines and incorporated into the acceptable use policy.
- By June 1, 2007, each division must send a statement to the director of the Office of Educational Technology confirming the completion of this work.
- During school year 2007-2008, each division will review the progress and effectiveness of its acceptable use policy and the implementation of its Internet safety program.
- By September 1, 2008, each division must submit to the Office of Educational Technology a copy of the acceptable use policy, including the Internet safety component and a statement that the policy and Internet safety program have been reviewed.
- In September 2008, the Office of Educational Technology will review each division's acceptable use policy and related Internet safety program description to determine the degree to which the expectations of *Code* §22.1-70.2 have been addressed.

The Office of Educational Technology developed the following rubrics to assist division superintendents with reviewing acceptable use policies. Each rubric defines the degree to which each division has adapted its acceptable use policy and implemented an Internet safety program, as mandated in §22.1-70.2.

Division Implementation Rubric for §22.1-70.2 Acceptable Internet use policies for public and private schools. (1999, c. 64; 2001, c. 269; 2006, cc. 52, 474.)

Code Requirement	Meets Expectations	Progress toward Expectations	Below Expectations
A. Every two years, each division superintendent shall file with the Superintendent of Public Instruction an acceptable use policy (AUP), approved by the local school board, for the Internet.	Documentation validates that every two years, the division superintendent has filed with the Superintendent of Public Instruction an AUP, approved by the local school board, for the Internet.	Documentation indicates that the division superintendent is in the process of revising the division's AUP. To date, the revised AUP document has not been filed with the Superintendent of Public Instruction.	Documentation is not available to validate that the division superintendent files with the Superintendent of Public Instruction an AUP.
At a minimum, the policy shall contain provisions that (i) are designed to prohibit use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet.	The AUP contains provisions to prohibit use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet.	The AUP contains provisions to prohibit use by division employees and students of the division's computer equipment for illegal actions. However, the definition of illegal use is not specified to include sending, receiving, viewing, or downloading illegal material via the Internet.	The AUP does not contain provisions to prohibit use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet.
At a minimum, the policy shall contain provisions that (ii) seek to prevent access by students to material that the school division deems to be harmful to juveniles as defined in §18.2372.	The division's policy contains provisions that seek to prevent access by students to material that the school division deems to be harmful to juveniles as defined in §18.2372.	The division's policy contains a statement that the division will seek to prevent access by students to material that the school division deems to be harmful to juveniles as defined in §18.2372. However, the statement does not identify specific provisions to prevent student access to harmful material.	There is no evidence that the division seeks to prevent access by students to material the school division deems to be harmful to juveniles as defined in §18.2372.
At a minimum, the policy shall contain provisions that (iii) select a technology for the division's computers having Internet access to filter or block Internet access through such computers to child pornography as set out in §18.2-374.1:1 and obscenity as defined in §18.2-372.	The division's policy contains provisions that identify a selected technology for its Internet-accessible computers to filter or block access to child pornography as set out in §18.2-374.1:1 and obscenity as defined in §18.2-372.	The division's policy contains a statement addressing the need for Internet filtering. However, provisions are not provided for the selection of a filtering and blocking technology.	There is no evidence of the division filtering or blocking Internet access to child pornography as set out in §18.2-374.1:1 and obscenity as defined in §18.2-372.
At a minimum, the policy shall contain provisions that (iv) establish appropriate measures to be taken against persons who violate the policy.	Appropriate measures are clearly defined for persons who violate the policy. The policy references federal legislation and Virginia state laws regulating Internet safety.	Measures are not clearly defined for persons who violate the policy.	The policy does not establish appropriate measures to be taken against persons who violate the policy.
The 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.	**OPTIONAL** Divisions are encouraged to provide appropriate evidence for additional terms, conditions, and requirements as deemed appropriate by the division for inclusion in the local policy. The division's policy should correlate with local Continuity of Operations Plan (COOP).	N/A	N/A
B. The superintendent shall take steps as he deems appropriate to implement and enforce the division's policy.	The division superintendent has clearly defined and taken steps deemed appropriate to implement and enforce the division's policy.	The division's policy is currently under development. Implementation has not taken place to date.	The division superintendent has not defined steps deemed appropriate to implement and enforce the division's policy.

Division Implementation Rubric for §22.1-70.2 Acceptable Internet use policies for public and private schools – (v) *a component on Internet safety that is integrated in a division's instructional program.* (1999, c. 64; 2001, c. 269; 2006, cc. 52, 474.)

Program Criteria	Meets Expectations	Progress toward Expectations	Below Expectations
The AUP Internet safety program contains a descriptive statement(s) regarding the division's instructional philosophies and strategies to be supported by Internet access in schools.	The program contains a statement(s) regarding the division's instructional philosophies and strategies to be supported by Internet access in schools.	The program contains a general statement(s) regarding the division's instructional strategies to be supported by Internet access in schools; however, it is unclear how Internet access relates to the philosophies and strategies.	The program contains no statement(s) regarding the division's instructional philosophies and strategies to be supported by Internet access in schools.
The AUP Internet safety program specifies the roles and responsibilities for division personnel (including but not limited to administrators, teachers, counselors, instructional technology resource teachers, library media specialists, building resource officers, and information technology coordinators) and students with regard to the acceptable use of electronic-based resources and Internet safety. An overview and outline of the program is available in electronic format for all to view.	The program clearly defines roles and responsibilities for all division personnel and students. There is an established schedule for the review of roles and responsibilities. Adjustments are made as needed. A current overview and outline of the program is available in electronic format for all to view.	The program defines roles and responsibilities for all division personnel and students; however, it is unclear if these roles and responsibilities have been reviewed periodically. AND/OR The program includes roles and responsibilities for a limited number of division personnel and students; however, it fails to identify or specify the roles and responsibilities for all appropriate division personnel.	The program does not identify roles and responsibilities for any division personnel or students.
The AUP Internet safety program specifies roles and responsibilities for community stakeholders with regard to the acceptable use of electronic-based resources and Internet safety.	The program specifies roles and responsibilities for community stakeholders. Mechanisms are in place for stakeholder feedback during the evaluation process.	The program specifies roles and responsibilities for community stakeholders. Stakeholder feedback is not addressed. AND/OR The program identifies community stakeholders but not their roles or responsibilities.	The program does not identify community stakeholders.
The AUP Internet safety program specifies safety measures in place, including filtering and monitoring procedures. The plan identifies measures for future implementation.	The filtering and monitoring procedures address current issues of concern. Procedures are reviewed and evaluated on a regular basis. The program outlines procedures for developing safety measures that will address emerging technologies not currently deployed in the system.	Procedures are reviewed and evaluated on a regular basis. However, there is no indication the reviews have resulted in follow-up actions or policy revisions. AND/OR The program does not outline procedures for developing safety measures that will address emerging technologies not currently deployed in the system.	Current filtering and monitoring procedures have not been reviewed.
The AUP Internet safety program describes methods by which the division ensures data and network security. The division's policy should correlate with local Continuity of Operations Plan (COOP).	Methods to ensure data and network security have been reviewed annually. Any present and potential problems have been identified, evaluated, and addressed.	Methods to ensure data and network security have been reviewed annually. There are no apparent plans for addressing potential problems.	Methods to ensure data and network security have not been reviewed.

Program Criteria	Meets Expectations	Progress toward Expectations	Below Expectations
The AUP Internet safety program describes technology-based applications and hardware prohibited for employee and student use. It identifies associated penalties.	Prohibited uses of technology-based applications and hardware within the division have been identified. Infractions are reviewed promptly as they occur. Stated penalties are enforced.	Prohibited uses of technology-based applications and hardware within the division have not been identified or reviewed as they occur. AND/OR Stated penalties have not been enforced consistently.	Prohibited forms of technology-based applications and hardware have not been identified.
The AUP Internet safety program describes procedures to address breaches of Internet and intranet security and safety. Legal actions resulting from breaches have been reviewed.	The program clearly defines procedures that address security and safety breaches. Legal issues have been reviewed, with appropriate information incorporated. The procedures address issues ranging from minor infractions to catastrophic events.	The spectrum of issues is narrow and does not include the full scope of potential problems. AND/OR Appropriate personnel have not reviewed legal issues.	Procedures to address breaches of Internet and intranet security and safety do not exist.
The AUP Internet safety program describes ongoing professional development opportunities for each stakeholder group. It includes an overview of both the needs assessment and evaluation processes for professional development and community outreach programs.	Professional development opportunities have been developed based on a needs assessment conducted for each group of stakeholders. Professional development is consistent with the program's goals. An evaluation process focuses on the role of professional development in the level of effectiveness for Internet safety and community outreach programs.	It is unclear if a needs assessment has been conducted or if professional development offerings and resources are consistent with the program goals. Evaluation procedures are unclear or not evident.	No professional development plans have been made for any stakeholder group.
The AUP Internet safety program describes community outreach activities that are consistent with the program's goals. It includes an overview of both the needs assessment and evaluation processes for community outreach programs.	Specific events and resources have been developed and/or provided based on a needs assessment of the community members. The events and resources are consistent with the program's goals. An evaluation plan focuses on program improvement.	It is unclear if a needs assessment has been conducted or if outreach activities and resources are consistent with the program's goals. Evaluation procedures are unclear or not evident.	There is no evidence of community outreach.
The AUP Internet safety program describes the division's procedures for the evaluation and revision of the AUP, including the Internet safety program.	The program includes an evaluation plan that addresses five areas of concern: accountability, effectiveness, impact, operations, and utility. Revision procedures are clearly outlined and realistically scheduled.	The program describes program evaluation procedures but does not consider all areas of concern: accountability, effectiveness, impact, operations, and utility. AND/OR Revision procedures are unclear.	Procedures do not exist for evaluating and revising the program and policy.
The AUP and Internet safety program have been implemented, enforced, evaluated, and adjusted when needed.	The AUP and Internet safety program have been presented to and approved by the local school board. Programs have been implemented, enforced, and evaluated following procedures outlined in the plan. Programs and policy have been adjusted as needed.	Planning has occurred, and the division is in the initial stages of implementation; however, it is unclear if the policy is being enforced or if revisions are being made as needed.	The AUP and Internet safety program have not been implemented, enforced, evaluated, or adjusted.

Appendix D

Number of Divisions in Each Category of the Compliance Rubrics

Number of Divisions in Each Category of the Compliance Rubrics

Code Requirement	*Meets Expectations*	*Progress towards Expectations*	*Below Expectations*
A. Every two years, each division superintendent shall file with the Superintendent of Public Instruction an acceptable use policy (AUP), approved by the local school board, for the Internet.	Documentation validates that every two years, the division superintendent has filed with the Superintendent of Public Instruction an AUP, approved by the local school board, for the Internet.	Documentation indicates that the division superintendent is in the process of revising the division's AUP. To date, the revised AUP document has not been filed with the Superintendent of Public Instruction.	Documentation is not available to validate that the division superintendent files with the Superintendent of Public Instruction an AUP.
NUMBER OF DIVISIONS REPORTED	**130**	**0**	**2**
At a minimum, the policy shall contain provisions that (i) are designed to prohibit use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet.	The AUP contains provisions to prohibit use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet.	The AUP contains provisions to prohibit use by division employees and students of the division's computer equipment for illegal actions. However, the definition of illegal use is not specified to include sending, receiving, viewing, or downloading illegal material via the Internet.	The AUP does not contain provisions to prohibit use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet.
NUMBER OF DIVISIONS REPORTED	**132**	**0**	**0**
At a minimum, the policy shall contain provisions that (ii) seek to prevent access by students to material that the school division deems to be harmful to juveniles as defined in §18.2-372.	The division's policy contains provisions that seek to prevent access by students to material that the school division deems to be harmful to juveniles as defined in §18.2-372.	The division's policy contains a statement that the division will seek to prevent access by students to material that the school division deems to be harmful to juveniles as defined in §18.2-372. However, the statement does not identify specific provisions to prevent student access to harmful material.	There is no evidence that the division seeks to prevent access by students to material the school division deems to be harmful to juveniles as defined in §18.2-372.
NUMBER OF DIVISIONS REPORTED	**132**	**0**	**0**
At a minimum, the policy shall contain provisions that (iii) select a technology for the division's computers having Internet access to filter or block Internet access through such computers to child pornography as set out in §18.2-374.1:1 and obscenity as defined in §18.2-372.	The division's policy contains provisions that identify a selected technology for its Internet-accessible computers to filter or block access to child pornography as set out in §18.2-374.1:1 and obscenity as defined in §18.2-372.	The division's policy contains a statement addressing the need for Internet filtering. However, provisions are not provided for the selection of a filtering and blocking technology.	There is no evidence of the division filtering or blocking Internet access to child pornography as set out in §18.2-374.1:1 and obscenity as defined in §18.2-372.

NUMBER OF DIVISIONS REPORTED	**132**	**0**	**0**
At a minimum, the policy shall contain provisions that (iv) establish appropriate measures to be taken against persons who violate the policy.	Appropriate measures are clearly defined for persons who violate the policy. The policy references federal legislation and Virginia state laws regulating Internet safety.	Measures are not clearly defined for persons who violate the policy.	The policy does not establish appropriate measures to be taken against persons who violate the policy.
NUMBER OF DIVISIONS REPORTED	**132**	**0**	**0**
The 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.	**OPTIONAL** Divisions are encouraged to provide appropriate evidence for additional terms, conditions, and requirements as deemed appropriate by the division for inclusion in the local policy. The division's policy should correlate with local Continuity of Operations Plan (COOP).	N/A **Numbers not collected for this item**	N/A
NUMBER OF DIVISIONS REPORTED			
B. The superintendent shall take steps as he deems appropriate to implement and enforce the division's policy.	The division superintendent has clearly defined and taken steps deemed appropriate to implement and enforce the division's policy.	The division's policy is currently under development. Implementation has not taken place to date.	The division superintendent has not defined steps deemed appropriate to implement and enforce the division's policy.
NUMBER OF DIVISIONS REPORTED	**132**	**0**	**0**
The AUP Internet safety program contains a descriptive statement(s) regarding the division's instructional philosophies and strategies to be supported by Internet access in schools.	The program contains a statement(s) regarding the division's instructional philosophies and strategies to be supported by Internet access in schools.	The program contains a general statement(s) regarding the division's instructional strategies to be supported by Internet access in schools; however, it is unclear how Internet access relates to the philosophies and strategies.	The program contains no statement(s) regarding the division's instructional philosophies and strategies to be supported by Internet access in schools.
NUMBER OF DIVISIONS REPORTED	**132**	**0**	**0**
The AUP Internet safety program specifies the roles and responsibilities for division personnel (including but not limited to administrators, teachers, counselors, instructional technology resource teachers, library media specialists, building resource officers, and information technology coordinators) and students with regard to the acceptable use of	The program clearly defines roles and responsibilities for all division personnel and students. There is an established schedule for the review of roles and responsibilities. Adjustments are made as needed. A current overview and outline of the program is available in electronic format for all to view.	The program defines roles and responsibilities for all division personnel and students; however, it is unclear if these roles and responsibilities have been reviewed periodically. AND/OR The program includes roles and responsibilities for a limited number of division personnel and students; however, it fails to identify or specify the roles and	The program does not identify roles and responsibilities for any division personnel or students.

electronic-based resources and Internet safety. An overview and outline of the program is available in electronic format for all to view.		responsibilities for all appropriate division personnel.	
NUMBER OF DIVISIONS REPORTED	**63**	**67**	**2**
The AUP Internet safety program specifies roles and responsibilities for community stakeholders with regard to the acceptable use of electronic-based resources and Internet safety.	The program specifies roles and responsibilities for community stakeholders. Mechanisms are in place for stakeholder feedback during the evaluation process.	The program specifies roles and responsibilities for community stakeholders. Stakeholder feedback is not addressed. AND/OR The program identifies community stakeholders but not their roles or responsibilities.	The program does not identify community stakeholders.
NUMBER OF DIVISIONS REPORTED	**47**	**69**	**16**
The AUP Internet safety program specifies safety measures in place, including filtering and monitoring procedures. The plan identifies measures for future implementation.	The filtering and monitoring procedures address current issues of concern. Procedures are reviewed and evaluated on a regular basis. The program outlines procedures for developing safety measures that will address emerging technologies not currently deployed in the system.	Procedures are reviewed and evaluated on a regular basis. However, there is no indication the reviews have resulted in follow-up actions or policy revisions. AND/OR The program does not outline procedures for developing safety measures that will address emerging technologies not currently deployed in the system.	Current filtering and monitoring procedures have not been reviewed.
NUMBER OF DIVISIONS REPORTED	**98**	**31**	**3**
The AUP Internet safety program describes methods by which the division ensures data and network security. The division's policy should correlate with local Continuity of Operations Plan (COOP).	Methods to ensure data and network security have been reviewed annually. Any present and potential problems have been identified, evaluated, and addressed.	Methods to ensure data and network security have been reviewed annually. There are no apparent plans for addressing potential problems.	Methods to ensure data and network security have not been reviewed.
NUMBER OF DIVISIONS REPORTED	**104**	**22**	**6**
The AUP Internet safety program describes technology-based applications and hardware prohibited for employee and student use. It identifies associated penalties.	Prohibited uses of technology-based applications and hardware within the division have been identified. Infractions are reviewed promptly as they occur. Stated penalties are enforced.	Prohibited uses of technology-based applications and hardware within the division have not been identified or reviewed as they occur. AND/OR Stated penalties have not been enforced consistently.	Prohibited forms of technology-based applications and hardware have not been identified.

NUMBER OF DIVISIONS REPORTED	**132**	**0**	**00**
The AUP Internet safety program describes procedures to address breaches of Internet and intranet security and safety. Legal actions resulting from breaches have been reviewed.	The program clearly defines procedures that address security and safety breaches. Legal issues have been reviewed, with appropriate information incorporated. The procedures address issues ranging from minor infractions to catastrophic events.	The spectrum of issues is narrow and does not include the full scope of potential problems. AND/OR Appropriate personnel have not reviewed legal issues.	Procedures to address breaches of Internet and intranet security and safety do not exist.
NUMBER OF DIVISIONS REPORTED	**39**	**90**	**3**
The AUP Internet safety program describes ongoing professional development opportunities for each stakeholder group. It includes an overview of both the needs assessment and evaluation processes for professional development and community outreach programs.	Professional development opportunities have been developed based on a needs assessment conducted for each group of stakeholders. Professional development is consistent with the program's goals. An evaluation process focuses on the role of professional development in the level of effectiveness for Internet safety and community outreach programs.	It is unclear if a needs assessment has been conducted or if professional development offerings and resources are consistent with the program goals.	No professional development plans have been made for any stakeholder group.
NUMBER OF DIVISIONS REPORTED	**66**	**66**	**0**
The AUP Internet safety program describes community outreach activities that are consistent with the program's goals. It includes an overview of both the needs assessment and evaluation processes for community outreach programs.	Specific events and resources have been developed and/or provided based on a needs assessment of the community members. The events and resources are consistent with the program's goals. An evaluation plan focuses on program improvement.	Evaluation procedures are unclear or not evident. It is unclear if a needs assessment has been conducted or if outreach activities and resources are consistent with the program's goals. Evaluation procedures are unclear or not evident.	There is no evidence of community outreach.
NUMBER OF DIVISIONS REPORTED	**58**	**66**	**8**
The AUP Internet safety program describes the division's procedures for the evaluation and revision of the AUP, including the Internet safety program.	The program includes an evaluation plan that addresses five areas of concern: accountability, effectiveness, impact, operations, and utility. Revision procedures are clearly outlined and realistically scheduled.	The program describes program evaluation procedures but does not consider all areas of concern: accountability, effectiveness, impact, operations, and utility. AND/OR Revision procedures are unclear.	Procedures do not exist for evaluating and revising the program and policy.

NUMBER OF DIVISIONS REPORTED	**44**	**88**	**0**
The AUP and Internet safety program have been implemented, enforced, evaluated, and adjusted when needed.	The AUP and Internet safety program have been presented to and approved by the local school board. Programs have been implemented, enforced, and evaluated following procedures outlined in the plan. Programs and policy have been adjusted as needed.	Planning has occurred, and the division is in the initial stages of implementation; however, it is unclear if the policy is being enforced or if revisions are being made as needed.	The AUP and Internet safety program have not been implemented, enforced, evaluated, or adjusted.
NUMBER OF DIVISIONS REPORTED	**63**	**69**	**0**

Appendix E

Summary of Pokémon Learning League Research Project

Summary of Pokémon Learning League Research Project

In 2006, Virginia enacted legislation—expanding upon a 2000 statute—requiring the Superintendent of Public Instruction to issue Internet safety guidelines to school divisions. In response, the Virginia Department of Education's Office of Educational Technology (OET) developed a guidance document to help educators integrate Internet safety into instruction. The overall approach was one of balance, recognizing the need to address the risks and highlight the benefits of Internet use in schools. The document demonstrated the Internet's unprecedented access to resources for enhancing learning, researching myriad topics, communicating, exploring new ideas, and expressing creativity. At the same time, it underscored that educators and students must understand the real, significant, and constantly changing dangers associated with the Internet.

In 2007, OET staff approached Pokémon Learning League to collaborate on the development of an entertaining and age-appropriate resource for teaching Internet safety to younger students. Beyond the obvious advantages of leveraging a cultural phenomenon to engage students, this online suite of standards-based animated interactive lessons in language arts, mathematics, science, and life skills was well designed and pedagogically sound.

The Pokémon Learning League team developed the storylines and storyboards, and the OET refined the content and recommended specific points about Internet safety. The OET reviewed the lessons and supporting resources through each step of the development cycle. This collaborative process produced the Web-based *Internet Safety and You* unit, which includes four lessons featuring an animated episode, guided practice, and a quiz. Each lesson addresses a distinct aspect of Internet safety. Other sections suggest additional resources for teachers and parents. Each lesson is aligned with Virginia's *Guidelines and Resources for Internet Safety in Schools*, which encourages teachers to integrate the program into their curricula (Virginia Department of Education, 2007).

To document any changes that the program made in student behavior, a survey was used with the students. A pretest/posttest design was used. The instrument consisted of 31 items, 19 of which were designed to ascertain students' knowledge about various Internet safety issues and gauge what they would do, or advise a friend to do, when encountering a situation online. Questions focused on four primary issues: online safety, cyberbullying, distinguishing fact from opinion, and understanding media. Students read a brief statement describing a scenario they or their friend have encountered and selected from three responses: unsafe, safe, or neutral, which fell on a continuum between the other two choices. Students then explained their responses in a text box. Eight items gathered information about the students' Internet experience; four addressed demographic information.

OET secured 4,000 licenses for Pokémon Learning League, and the project was announced at the annual Educational Technology Leadership Conference in December 2007. Divisions that agreed to the project conditions were given free access to Pokémon Learning League for one year. The divisions had to identify a local coordinator, distribute and collect consent forms, ensure that all participating students complete an online

questionnaire prior to beginning the lessons, ensure that all students complete the Internet safety modules during the academic year, and ensure that all students complete a second questionnaire within two weeks of completing the modules. Twenty-one divisions and two schools from nonparticipating divisions participated in the project; six failed to complete the project.

The major findings led to three conclusions. First, a large number of the fourth graders demonstrated substantial knowledge about Internet safety even before the unit (e.g., 91.1% realized they should tell a trusted adult after receiving an e-mail that makes them uncomfortable), although a small but substantial number maintained risky attitudes even after the unit (e.g., 44 fourth graders [3.2%] reported they would check other links even after seeing an uncomfortable picture). Second, after the unit, students improved significantly in all 10 Internet safety aspects based on the χ^2 test results, with one exception—meeting friends in person. These tests indicated there were significant changes in the types of responses—from unsafe to safe—before and after the unit. Third, student responses to the 10 scenarios differed significantly. For example, before taking the unit, 50 students (3.6%) said they would meet an Internet stranger in person; after the unit, the improvement was minimal—34 students (2.5%).