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.