Model Policy Concerning Internet Safety

CONTENTS

INTRODUCTION

A. To emphasize the essential role of technologies in the learning experiences of students, the Virginia Department of Education (VDOE) is committed to helping school boards develop and implement internet safety policies and programs. Safeguarding students remains the utmost priority, even though the task may seem formidable. Leaders must actively address this imperative. The dynamic evolution of the internet underscores the significance of this responsibility for all community members.

PURPOSE

A. The Department developed the "Model Policy Concerning Internet Safety" in response to § 22.1-24.1. Internet Safety Advisory Council with input as required by the law from individuals and organizations throughout the Commonwealth and beyond. It represents the knowledge and perspectives of teachers, researchers, law enforcement, nonprofit organizations, as well as local, state, and federal representatives. The purpose of this council is to advance the goal of safe use of media and technology by students and teachers in public elementary and secondary schools in the Commonwealth. This document has been developed for local school boards in the Commonwealth to enable such school boards to better ensure the internet safety of all students and teachers in the local school division. While this document offers recommendations, specific integration details are left to the discretion of local education agencies.

DEVELOPMENT

A. Section 22.1-24.1 of the Code of Virginia provides that the Superintendent of Public Instruction "shall establish and appoint members of the Internet Safety Advisory Council (the Council) for the purpose of advancing the goal of safe use of media and technology by students and teachers in public elementary and secondary schools in the Commonwealth." The statute sets out the membership of the Council. This section of

Code was added by Chapter 776 during the 2022 General Assembly. Chapter 111 (2023 Acts of Assembly) amended this section to add that the Council may collaborate with law enforcement agencies, criminal justice agencies, and other non-governmental organizations with expertise in child online safety issues and human trafficking prevention. The statute is in effect until July 1, 2024.

B. The duties of the Council include:
   1. Developing recommendations to the Board of Education for adoption, a model policy for local school boards that would enable them to better support the internet safety of all students and teachers.
   2. Developing recommendations to the Board of Education for adoption, model instructional practices for and instructional content on the safe use of media and technology by students and teachers.
   3. Designing and posting on the Department's website a page with links to successful instructional practices, curricula, and other teacher resources.

C. The Council met beginning in September 2023 and concluded in 2024.

GUIDING PRINCIPLES

A. In an environment of constrained resources, school leaders leverage security investments to focus on the most impactful steps. Schools are responsible for protecting student privacy on school devices and networks by implementing appropriate security measures.

B. Education is essential in supporting the safety of children. Educators integrate digital wellness skills into the core curriculum teaching students to help students navigate modern technology in a healthy and productive manner including the most common online threats and ways to respond.

C. Internet safety training at school will impact student behavior on the personal devices for accessing the internet, including mobile phones.

D. Law enforcement focus on collaboration and information sharing with local school divisions.

E. Local school boards invest in building teacher capacity through systematic, high quality professional learning opportunities.

F. While no comprehensive list exists to cover all situations, appropriate safe, legal, and ethical online behavior should include the following:
    a. Protecting your personal information online.
    b. Using strong, unique passwords for different accounts and enable two-factor authentication whenever possible.
    c. Avoid clicking on suspicious links or downloading files from untrusted sources.
    d. Treating others with respect in online interactions.
    e. Obeying copyright laws.
    f. Respecting intellectual property rights, defamation laws, and privacy regulations.
    g. Following community guidelines on social media platforms, forums, and websites.
    h. Curating reliable sources and fact-checking claims to promote accurate knowledge.
    i. Reporting illegal content (such as child exploitation or hate speech) to the appropriate authorities.

RELATED LAWS

A. The policy must comply with current federal, state, and local laws relating to internet safety.
    a. Federal Laws:
        i. Federal Educational Rights and Privacy Act (FERPA)
        ii. Children's Online Privacy Protection Act (COPPA)
        iii. Protection of Pupil Rights Amendment (PPRA)
        iv. Individuals with Disabilities Act (IDEA)
        v. Rehabilitation Act: Section 504
        vi. Children Internet Protection Act (CIPA)
    b. Code of Virginia:
        i. Acceptable Use Policy
        ii. Students' personally identifiable information
        iii. Broadband services for educational purposes

iv. Instructional technology resource teachers and technical support
v. Integration of educational technology into instructional programs
vi. Professional development in the use of educational technology

PUBLICATION INFORMATION

Questions or inquiries about this document should be directed to:

Virginia Department of Education

Office of Policy: Department of Policy and Communications

Office of Educational Technology and Classroom Innovation: Associate Director

P.O. Box 2120 Richmond, Virginia 23218-2120

(804) 225-2092

APPENDIX 1

SAMPLE POLICY

The following Sample Policy is provided for consideration or use by local school boards as they develop and implement their policies in compliance with the Act.

I. Purpose:
   a. This document has been developed for local school boards in the Commonwealth to enable such school boards to better support the internet safety of all students and teachers in the local school division. While this document offers recommendations, specific integration details are left to the discretion of local education agencies.
   b. The VDOE encourages local education agencies to infuse digital access, use, and design practices as well as engage in conversations about digital citizenship and

internet safety as a critical component of supporting safety. School boards shall adopt policies to support safety. Leaders shall keep staff and community members apprised of the new policy. Parent resources may be curated by local school board advisory councils which may include resources and assistance programs available for any child or parent who may have encountered online solicitation by sexual predators or other illegal online communications or activities, including the National Center for Missing and Exploited Children's CyberTipline.

II. Definitions:

a. Internet Safety: the practice of following actionable guidelines, understanding modern technology, and protecting digital devices so users can defend against the malicious parts of the online world.
b. Digital Learning: to empower students as learners by improving their functional literacy as digital citizens capable of constructing knowledge, designing innovative works, thinking computationally, creatively communicating, and collaborating with others locally, regionally, and globally.
c. Digital Citizenship: the state of being skilled in using the internet in order to communicate with others in a safe and responsible way.
d. Media Literacy: the ability to access, curate, use, analyze, evaluate, create, and act using all forms of communication.
e. Social Media: websites and other online means of communication that are used by large groups of people to share information and to develop social and professional contacts.

III. Access to Educational Technology:

a. Where schools provide technology for student use, schools shall use tools and technologies to monitor, filter and limit use as part of the training and in accord with the law. For instance, internet filters shall be used to block or filter inappropriate information. This is required by the Children's Internet Protection Act (CIPA), whereby blocking shall be applied to visual depictions of material deemed obscene, child pornography, or any material deemed harmful to minors. As required by the CIPA, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities;

and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

b. It shall be the responsibility of all members of the staff to educate, supervise, and monitor appropriate usage of the online computer network and access to the internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

c. Local education agencies can prevent students from accessing social media platforms and other non-instructional applications through the use of internet access provided by the school.

d. After completing an introductory, age-appropriate training, the student will be provided internet access. The training provided will be designed to promote the school's commitment to:

    i. The standards and acceptable use of internet services as set forth in the acceptable use policy.

    ii. Student safety with regard to digital citizenship.

    iii. Compliance with the E-rate requirements of the CIPA.

e. The student will acknowledge receipt and understanding of this training and will follow the provisions of the acceptable use policies. Student acknowledgement should be provided in plain language that is age appropriate for the student.

IV. Use of Educational Technology:

a. Acceptable Use Policy: Local School Boards update existing acceptable use policies as required by § 22.1-70.2. that build skills in internet safety, media literacy and digital citizenship through access to the resources available on digital platforms that support inquiry-based education. The policy should be available in formats that are age appropriate, written in plain language, and easily accessible to students, educators, and families.

b. Advisory Group: Formal designation of a local school board advisory group, composed of parents, students, community members, educators, administrators, and law enforcement who are responsible for reviewing the code of conduct, acceptable use policy, and community resources to ensure a set of principles,

expectations, rules, and communication clarifies the expectations of digital citizenship, media literacy, and internet safety.

V. Design Instruction:

a. Strategic Planning: When planning, school leaders shall include digital citizenship into the school division's broader goals, especially in the areas of:

   i. The risks of transmitting personal information on the internet and the importance of privacy protection.

   ii. The enforcement of copyright laws on written materials, photographs, music, and videos posted or shared online.

   iii. The importance of establishing open communication with responsible adults about any online communications or activities.

   iv. How to recognize, avoid, and report suspicious, potentially dangerous, or illegal online communications or activities, including (a) potential solicitation by sexual predators, (b) unsolicited or deceptive communications, and (c) harassment and cyberbullying.

   v. Safe and responsible use of social networking websites, including the advantages of social media use, as well as the potential harms including addiction, publication of misinformation, negative effects on mental health, and the permanent nature of content created on social media.

b. Professional development: School divisions may work with local law enforcement and recognized educational organizations to inform teachers of the latest developments in the safe and effective use of media and technology with students.

c. Disclosure plan: School leaders shall provide teachers age-appropriate resources and assistance programs to share with any child or parent who may have encountered online solicitation by sexual predators or other illegal online communications or activities, including the National Center for Missing and Exploited Children's CyberTipline.

d. Digital Learning Integration Standards of Learning (DLI): School divisions are required to integrate the DLI into a broader, locally designed curriculum. All companion documents, activities performed, and approved technologies used in implementing the DLI should fall within the acceptable use, student conduct, and

all other school division policies. Educators are encouraged to document lessons which explicitly integrate the DLI into the curriculum.

e. Divisions should provide internet safety and digital citizenship resources to their school community including online courses, in person programs, resource hubs, and digital guides.