NBI SEMINAR--SCHOOL LAW: SOCIAL MEDIA AND APPS, CYBERBULLYING, PRIVACY AND OTHER TECHNOLOGY ISSUES

INTERNET ACCEPTABLE USE POLICIES, FILTERING AND MONITORING

LAPTOPS, TABLETS AND IPADS: LEGAL CONCERNS

Prepared by: Marcus A. Manos
Member (Also Admitted in NC and DC)
Nexsen Pruet LLC
Post Office Drawer 2426
Columbia, South Carolina 29202
(803) 253-8275
mmanos@nexsenpruet.com

For The National Business Institute Seminar December 14, 2017

The attached materials are for educational purposes only and do not constitute legal advice. In the event of a legal issue related to these subjects, the reader should not rely on these materials or the presentation but consult an attorney and receive advice based on the facts of the reader's situation.

INTERNET ACCEPTABLE USE POLICIES, FILTERING AND MONITORING

Internet based learning applications provide flexibility, ease of access, continuous updating, and effective instructional platforms for education institutions. Initially electronic devices came into schools as advanced note taking devices. The last two decades produced a revolution in interactive use of electronic devices. Many school districts, like Richland School District One here in Columbia, now provide student devices free of charge, except for an insurance coverage payment. Electronic devices are now an integral part of the instructional methods used in schools.

Electronic devices with access to the Internet and web based applications present unique challenges in the academic setting. The web provides excellent research sources, but also unreliable ones. Email communication between students and teachers provides instantaneous and easy to use document communication, but also poses system risks from viruses and other intrusions. Educational apps provide easily updated, less expensive and more versatile teaching tools than textbooks or workbooks, but students might be downloading much more that the approved apps. The South Carolina Department of Education's minimum standards of student conduct requires every school district to make it an offense to have a cell phone, table, iPad or computer in violation of school board policy, laying the legal foundation for acceptable use policies. S.C. Code Ann. Regs. R. 43-279.

Schools must respond with policies and technologies that:

(1) Protect students from unwanted/illegal/immoral materials;
(2) Keep students focused on the educational subjects;
(3) Protect against harassment and unwanted contact; and
(4) Provide proportionate and effective discipline to further these goals.

I. Effective Acceptable Use Policies.

A. Considerations for Drafting an Acceptable Use Policy.

The Internet contains many educational resources, but also many documents, images, and files not suitable for children. An acceptable use policy for teachers, staff, and students defines inappropriate materials and establishes what cannot be accessed as well as possible sanctions if violated. The policy should define 'acceptable use' of technology for educational purposes.

Design the policy to address risks. Some examples of common risks:

- Messages with sexual content going to/or coming from students;
- Access to sexually explicit or inappropriate violent content;
- Access to illegal sites or sites promoting/enabling illegal content;
- Contact with potential outside person who might be predators, dealers in illicit materials, or hackers;
- Transfer of personally identifiable information to persons without authority or need to see such information;
- Student behavior in the use of technology that distracts from the learning environment; and
- Dangerous or destructive student behavior enabled or implemented by the use of technology.

Risk analysis cannot stand alone, however. Every school, but particularly public schools must be aware of limits on governmental power to interfere with

students and staff constitutional and statutory rights. In drafting an acceptable use policy, consider:

- Free speech rights;
- Freedom of religious belief;
- Invasion of privacy from monitoring email and other communications (private employers who give employees access to employer owned systems need not worry about this, governmental entities must worry about it to a greater extent); and
- Legal obligations of the school to third parties for student behavior.

Often an acceptable use policy will consist of several elements. Employee handbooks govern administrators, teachers and staff with access to the school's systems or hardware. Student discipline policies should reflect the student responsibilities for use of and care of school technology. A stand-alone student acceptable use policy that links back to the disciplinary handbook will often be useful. Finally, a contract between parent, student and school regarding the use and protection of technology and systems brings in the final constituency, parents and guardians.

Any acceptable use policy requires certain basics.

- Clear definition of appropriate materials and resources;
- Clear definition of inappropriate materials and resources;
- Clear definition of appropriate electronic communications;
- Clear definition of inappropriate electronic communications;
- Describe the role, restriction on and responsibility of administrators, teachers and staff;
- Responsibilities of parents/guardians and students; and
- Process of determining violations and consequences of violations.

Because of the special role of school's in protecting students, the policy or contract should include "safety first" tips that would not normally appear in business policies. For example, warnings and instructions about things not to do and what a student should immediately disclose to parents. Taking the form of a pledge: "I will never agree to see someone I 'meet' online without first checking with my parents. If my parents allow me to see them, my mother or father will come with me and it will be at a public place." Lawrence J. Magrid wrote instructive guides for elementary and teenage students titled "My Rules for Online Safety" and "Teen Safety on the Information Highway" that can assist in thinking about safety issues for a policy.

The school must decide where the policy should fall on the spectrum between highly defined restrictions and open-ended guidance. One of the easiest policies to develop and enforce is the restricted content variety. The school provides a definitive, complete list of every app, resource and website a user may access. Often with this type of policy, the school deploys software programmed to prevent access outside the list. In designing a strict access only policy, the school must consider neutrality and purpose. For example, a policy that allows access only to websites affiliated with one political party but blocking all others or one religion while blocking all others will likely result in litigation about free speech or religious establishment.

Each employee of the school should sign acknowledging acceptance of their employee acceptable use policy and be given a copy. Each employee should also sign an acknowledgment of understanding and having the student acceptable use policy and the parent/student/school contract. A single office or employee should monitor the policy, keep it current, and keep copies of all the signed acknowledgements from staff, students, and parents. That same office ought to provide the hearing officer or vice principal responsible for investigation and enforcement.

One area many school policies do not address—guest users. Most governmental buildings and many private businesses now provide WiFi access for guests or customers. Schools usually operate in a more restricted environment, but guest speakers or lecturers, recruiters, and others do visit and may want to make use of the school's networks or technology. The school may want to develop a guest use policy as well.

Many schools today provide hardware, software, apps and networks for students. In that situation, the policy must also address care for and damage to school property. Mandatory insurance programs through the school help protect the school and the using families.

Any policy should receive both legal and technical review. Select an attorney knowledgeable about state and local laws and requirements.

B. The Law and Acceptable Use Policies.

Any school in South Carolina participating in a State Board of Education approved virtual education program must implement an acceptable use policy for the program. S.C. Code Ann. R. 43-358. The student and the parent/guardian must sign and accept the policy. *Id*.

In *Al Zeiny v. Washington Safety Mgt. Solutions, LLC,* a discharged employee sued his former employer for violating Title VII of the Civil Rights Act, 42 U.S.C. §§ 2000e-2000aa. Civ. Act. No. 1:09-2821 (D.S.C. March 2, 2012) (2012 WL 1098209). The Magistrate Judge recommended summary judgment for the defendant on all claims except hostile environment. In part, the recommendation relied on the company's acceptable use policy the employee violated by sending email out of the United States for personal purposes, in Arabic and encrypted. The policy required employees not to use company email for personal purposes, not to translate email into foreign languages without permission, and not to use any encryption other than that provided by the company.

A violation of a neutral Acceptable Use Policy that forbade Fed Ex employees from using the company system to falsify company documents defeated any claim of discrimination, as dismissal for an admitted violation of the policy was not pretext. This is a good example of how a properly drawn acceptable use policy can

protect an employer from liability. *Feaster v. Federal Express Corp.*, Civ. Act. No. 2:13-CV-2517 (D.S.C. Aug. 28, 2014) (2014 WL 4269082).

The court discussed the difficulties facing a public entity setting up a strict blocking regime in *Mainstream Loudoun v. Board of Trustees of Loudoun County Library*, 24 F.Supp.2d 552 (E.D. Va. 1998). The court found that the library (like a school) is not under any obligation to provide internet access to its patrons, but once it does the First Amendment restricts what limitation the library may put in place. *Id*. at 570. Any such policy must be: (1) necessary to further a compelling government interest (protection of children is usually considered one); (2) narrowly tailored; (3) should not restrict the access of adults just because the content is inappropriate for minors (not usually an issue for schools); (4) must have clear and adequate standards; and (5) have procedural safeguards for prompt review. The court found the library's use of strict content limiting software unconstitutional. *Id*. The lesson for schools is you must make sure all restrictions are necessary to protect children and the educational purpose. Also, there must be a review/appeal process that will make an adequate record for judicial review of any alleged violations.

C. Resources for Developing a Policy.

Armadillo's acceptable use policies
[http://www.rice.edu/armadillo/Rice/Resources/acceptable.html]
An extensive set of resources on acceptable use policies at Rice University.

ERIC's list of acceptable use resources
[gopher://ericir.syr.edu:70/11/Guides/Agreements]
A list of acceptable use resources.

GSN acceptable use policies
[http://www.gsn.org/web/tutorial/issues/aupsampl.htm#begin]
Another list of actual acceptable use policies at the Global SchoolNet Foundation.

K-12 acceptable use policies
[http://www.erehwon.com/k12aup/]
An excellent starting point by Nancy Willard at Internet Marketing Services for learning about acceptable use policies, including templates for students, employees, guests, etc.

http://www.educationworld.com/a_curr/curr093.shtml
Education World® introduction to AUP.

D. Here are a Few Samples of Real Work School Acceptable Use Policies:

1. I attach a copy of the Richland County School District One Digital Learning Environment Technology Handbook for Students and Parents received by one of my children last year. The Acceptable Use Policy appears at page 10 forward. This is a useful tool for a laptop provided program. **ATTACHMENT 1**.

2. Richland County School District One also devotes a portion of the Student Code of Conduct Handbook to Acceptable Use Policy of Information Systems (Policy IJNDB-R). **ATTACHMENT 2**.

3. Richland Lexington School District Five's Acceptable Use Agreement for All Students appears at **ATTACHMENT 3**. Note the cross reference to the Student Behavior Handbook.

4. I also attach a simple one page policy and agreement from Richland School District of Richland, Washington. **ATTACHMENT 4**.

II. Internet Filtering Requirements.

State and federal laws require persons making the internet available to minors protect them from inappropriate content. Schools must be aware of the statutes, regulations and court decisions defining these legal requirements. Schools should design systems and policies complying with legal safe harbor requirements, as a protection against liability.

A. The Children's Internet Protection Act (CIPA) 42 U.S.C.A. §§ 254(h) and 254(l).

CIPA requires any school providing internet access to have a safety program, certify that program to the FCC, and defines content that is harmful to minors. The Supreme Court of the United States upheld CIPA from constitutional challenge by the American Library Association in *U.S. v. American Library Ass'n*, 539 U.S. 194 (2003). The school also needs to be aware of the Neighborhood Internet Protection Act (NCIPA) enacted at the same time and impacts schools and libraries as well.

The law requires K-12 schools and libraries to use internet filters and implement a safety policy to protect children from harmful internet content. CIPA defines harmful to minors as:

> Any picture, image, graphic image file, or other visual depiction that – (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;

and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

The FCC produced a simple explanatory pamphlet regarding CIPA, I attach as **ATTACHMENT 5**. If your school is just now providing internet access, please note there is a public hearing requirement before implementing the proposal.

B. The Complexity of Filtering.

Schools face a daunting employment market for professionals who can monitor and customize filters. The level of skill and the complexity of the work is illustrated in a recent case where a school district network engineer responsible for the filtering system failed to win an overtime claim because the court found him to be a an expert computer engineer exempt from the Fair Labor Standards Act. *Campbell v. Kannapolis City Schools Bd. of Educ.*, 55 F.Supp.3d 821 (M.D.N.C. 2014).

There are several good commercial filtering products out there. Each requires engineer level monitoring, customization and updating to meet the goals of the school district. While I do not recommend a specific product, I have seen each of the following in operation at clients or school districts:

- X-Stop by Log-On Data Corp.;
- Solarwinds Remote Monitoring & Management;
- GoGuardian for Chromebooks;
- iPrism Secure Web Gateway by EdgeWaver;
- Zscaler Web Filtering;
- Umbrella by Cisco;
- Web Filer Longhorn by Lightspeed Systems;

- WebTitan Cloud;
- Untangle; and
- [Content]Watch for Education.

Legacy web filters can be ineffective and inflexible when it comes to allocating what network resources users, apps and devices can access. An out-of-date systems provide only basic block/allow port and url-based functionality. An inflexible or out dated filter can put CIPA Compliance and E-Rate Funding at risk.

Many of the most popular filters run as hardware based web-filtering appliances. Some of these are not truly school oriented and they all tend towards being expensive and requiring significant effort to install, customize, and operate. Browser extensions and cloud based filtering may provide cheaper and more flexible solutions. The school district may use a solution-based request for proposals (RFP), seeking the best and least expensive solution. A committee representing technical, teaching and security resources can evaluate whether a solution meets all needs. By not particularizing the RFP toward a specific type of technology, the committee can compare various approaches. Note that a fair can competitive bidding process is required for using Universal Service Fee funds. 47 C.F.R. §54.503.

Whenever a school district looks for a new web filter, remember the E-Rate Funding, available through the FCC, can cover some of the cost. The person responsible for the project needs to become familiar with the E-Rate Funding regulations. 47 C.F.R. §§ 54.500 to 54.523. The Universal Service Administration

Company administers this program providing a funding source for schools and libraries.

This January 2017 article in EdTech Magazine gives some excellent insights. https://edtechmagazine.com/k12/article/2017/01/law-requires-content-filtering-school-and-library-networks.

III. Regulating and Monitoring Computer Use.

You now have a policy on computer use and understand the law applicable to internet filtering. The next step must be finding ways to enforce the policies adopted by the school or district. This step requires near real time monitoring of use, device tracking, and reasonable regulations. Each of these components can trigger privacy and expression concerns that will be discussed in another section.

A. Tracking Your Hardware.

In a four-month period in 2008, the Memphis City Schools had 1,800 laptops lost, stolen, or destroyed.[1] Because the district used a policy with required insurance, it suffered no losses due to the laptop hardware, but it did have to replace software and data. I imagine premiums increased the next year as well.

The key steps in a hardware protection program begin with good, old-fashioned property marking/tagging. Begin by assigning each laptop, notebook, projector, hard-drive etc., an identifying alphanumeric label with a bar code. Use an

[1] Snyder, Tara, "How to Keep School Laptops Safe", Edutopia, April 1, 2009

attaching plate or label that is difficult to remove. Follow this by laser etching the school or district name, warning it is school property and purchasing it from anyone other than the school or district may be a criminal act and the school will prosecute or sue.

PROPERTY OF NIMROD SEMI-PUBLIC SCHOOLS
Possession by Anyone Not Authorized by Nimrod May be a Crime and Nimrod Will Prosecute or Sue Violators

The Putnam Valley Central School District in New York began such a laser-marking program and reduced laptop loss.[2] Laser markers are expensive, some of the medical equipment grade models are prohibitively expensive, but they can be acquired for between $8,000 and $11,000 and the markings seem to deter theft and lead to the return of lost machines.

Next, install tracking software on the laptops. Most everyone knows "Find My iPhone" and how it works. Schools can purchase sophisticated software to track laptops. Products like Computrace, MyLaptopGPS, EXO5, PreyProject, Norton Anti-Theft, LockItTight, Stealth Signal and PC Phone Home may work for your school or district. Studies show these applications pay for themselves in reduced losses and returned machines in a short time frame.

Above we discuss the need to have a single administrator in charge of acceptable use policy maintenance and collecting signed copies. Likewise, one IT

[2] Id.

resource should be in charge of hardware inventory, labeling, marking, tracking and recovery. An accurate, real time updated inventory and marking program lies at the core of hardware protection. Tracking software must be frequently updated and monitored. The program director must keep track of new developments in tracking and recovery technology. Criminals continuously develop removal and work around tools to disable trackers. You can only protect your property if you are up to date on these issues.

Another possible protection is remote control/wipe functionality. This allows the administrator to wipe the machine to protect valuable data. These applications are very popular with professional firms to protect client data and confidential work product. The best applications are very expensive and may not be cost efficient for schools that do not have much proprietary or business data at risk.

B. Insurance is a Must!

Insurance against burglary, theft, vandalism and many kinds of damage to laptops exists in the marketplace. The more comprehensive the insurance protection, the more expensive the policy. Many Original Equipment Manufacturers (OEM) have insurance or extended warranty programs. When issuing a RFP for laptops, request that the OEM provide information on any extra warranty or insurance programs it may offer. Safeware, Inc., DataSecurity.com, Asurion, eSURRANTY,

Worth Ave. Group, and other specialty insurers provide this type of coverage as well as some mainstream insurance companies.

Many schools and districts require the parent or guardian to pay for the insurance. In Richland School District One, the insurance is $30 per school year.

C. Monitoring.

I discuss filtering software above. Even if the school or district uses filtering software, it should install monitoring software on all laptops. Monitoring products can be restricted to internet usage or provide every application, communication, and surfing activity done on the computer. Once again the more comprehensive the product the more expensive it tends to be. In evaluating monitoring applications, pay attention to the ease of extracting and reporting information. Reports need to be at a level they are easily understood. GFI WebMonitor, CurrentWare, PRTG, VictorOps aned Veriato 360 monitor web use, sites visited and time spent on the internet. You need to have a policy of how often you will check the reports and a process for random review. One can use these packages to place time restrictions on the computer to limit communication during certain hours. Vendors designed these programs for monitoring employees, but similar principles apply to students.

If you allow your students to use school email or even their own email accounts on school laptops, some form of email monitoring should be employed to meet the school or district's obligation to protect its students. These applications

deploy controls as well as monitoring functions. Among the products available: TERAMIND, Veriato, SentryPC, NetVizor, InterGuard, workexaminer, StaffCDP, OsMonitor, iMonitorSoft, and Pearl Software.

In addition to monitoring internet and other usage, consider software that prevent installation of programs, downloads, or acts as a gatekeeper to what type of software can run on the machine. Deep Freeze and Shadow Defender limit downloads or installations. Other applications provide application whitelisting (AWL) selecting applications that can run on the laptop rather than trying to blacklist or ban applications. I attach the National Institutes of Standards and Technology's "Guide to Application Whitelisting" NIST Special Publications 800-167 as **ATTACHMENT 6**. This guide explains the methodology and purpose of whitelisting and is part of NIST's Computer Security Series.

Bit9 Parity, Coretrace Bouncer, Faronics Anti-Executable, Lumension Application Control, McAfee Application Control, Microsoft AppLocker, and Savant Protector provide application control and "white listing" features. While presenting its own challenges, managing access by listing only the applications and features allowed tends to be much easier than an ever-changing list of forbidden features.

D. Discipline for Inappropriate Email/Accessing Inappropriate Content.

Now that your monitoring applications produce readable, comprehensive reports on what students and staff do with school computers, you need a policy on how to spot check, second review, and use the data. Ultimately, the policy will produce instances that appear to violate the Acceptable Use Policy. The monitoring official should turn the data over to the enforcing official discussed in Section I above. The enforcement official then investigates and calls in the student or the student and parent/guardian depending on the severity of the offense.

Discipline should follow the normal discipline handbook procedures and severity levels. The most serious offenses will require a hearing. I attach a notice memo used by a high school in Utah that might make a good starting point for a similar form in your school. **ATTACHMENT 7**.

The use of technology for blackmail, sexual solicitation, bullying and other illegal conduct needs swift and severe consequences. When students bypass filters and controls, the administration must undertake an investigation to determine how and then improve security.

Schools may discipline students for electronic misconduct. A disabled student convinced a friend to place a threatening electronic note in another student's computer file in *Wilson v. Fairfax County School Board*, 372 F.3d 674 (4th Cir. 2004). The email read "DEATH AWAITS YOU." The school disciplined the

student and transferred him to a different elementary school for disciplinary problems. The student who suffered from ADHD sued alleging a violation of the Individuals with Disabilities Education Act (IDEA) "stay-put" provision requiring schools to accommodate disabled students in their current educational environment. The court found the disability did not factor into the misconduct and that the student knew the wrongful nature of the electronic threat. The appeals court affirmed dismissal of the case.

School discipline for electronic offenses can trigger First Amendment concerns. *Coy v. Board of Educ. of North Canton City Schools*, 205 F.Supp.2d 791 (N.D. Ohio 2002). In that case, a student accessed an unauthorized website on a school issued laptop during class, but did so occasionally and in a manner to draw as little attention as possible to what he was viewing and did not display it to other students. The student designed the website himself. He was suspended and then expelled for a total of 84 days. His parents sued saying the school acted because school officials did not like the content of the student's personal website, not because of his on class period of quiet violations. The court described the website:

Before March 2001, Jon Coy created a website. He created the website on his home computer, and he created it on his own time. No part of his website was created using school equipment or during school hours.

> Jon Coy's website purported to describe the exploits of a group of skate boarders who called themselves "NBP." The website contained pictures and biographical information of Coy and his friends, quotes attributed to Coy and his friends, and a section entitled "losers." The "losers" section contained the pictures of three boys who attended the North Canton Middle School. A few insulting sentences were written under each picture. Most objectionable was a sentence describing one boy as being sexually aroused by his mother. In addition to the "losers" section, the website contained two pictures of boys giving the "finger," some profanity, and a depressingly high number of spelling and grammatical errors. While somewhat crude and juvenile, the website contains no material that could remotely be considered obscene.

The court applied the following principles in refusing summary judgment and requiring a trial on the First Amendment claims:

> Courts have long held that students do not "shed their constitutional rights to freedom of speech or expression at the schoolhouse gate." *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503, 506, 89 S.Ct. 733, 21 L.Ed.2d 731 (1969). However, it is equally clear that public school officials have the right to regulate speech "in the classroom or in school assembly" and "prohibit the use of vulgar and offensive terms in public discourse." *Bethel Sch. Dist. No. 403 v. Fraser*, 478 U.S. 675, 683, 106 S.Ct. 3159, 92 L.Ed.2d 549 (1986). Students' first amendment rights "must be 'applied in light of the special characteristics of the school environment.'" *Hazelwood Sch. Dist. v. Kuhlmeier*, 484 U.S. 260, 266, 108 S.Ct. 562, 98 L.Ed.2d 592 (1988) (quoting *Tinker*, 393 U.S. at 506, 89 S.Ct. 733). Importantly, "[a] school need not tolerate student speech that is inconsistent with its 'basic educational mission,' even though the government could not censor similar speech outside the school." *Id.* (quoting *Fraser*, 478 U.S. at 685, 106 S.Ct. 3159).
>
> In *Tinker*, the Supreme Court considered a school district's suspension of students who violated school policy by wearing black armbands to school in protest of the Vietnam War. The Court held that the school's actions violated the students' freedom of speech. *Tinker*, 393 U.S. at 513–14, 89 S.Ct. 733. The Court noted that "[t]he problem posed by the present case does not relate to regulation of the length of skirts or

> the type of clothing, to hair style or deportment .... Our problem involves direct, primary First Amendment rights akin to 'pure speech.' "*Id.* at 507–08, 89 S.Ct. 733. The Court concluded that to justify the prohibition of a particular expression of opinion, the school must "show that its action was caused by something more than a mere desire to avoid the discomfort and unpleasantness that always accompany an unpopular viewpoint." *Id.* at 509, 89 S.Ct. 733. The Court held that the prohibition of the armbands could not be sustained without showing that engaging in the prohibited conduct would "materially and substantially interfere with the requirements of appropriate discipline in the operation of the school." *Id. (*quoting *Burnside v. Byars*, 363 F.2d 744, 749 (5th Cir.1966)).
>
> In *Fraser*, the Supreme Court distinguished *Tinker* when it held that a school district acted within its permissible authority in disciplining a student who gave an offensively lewd and indecent student government nomination speech at a mandatory school assembly. *Fraser*,478 U.S. at 685, 106 S.Ct. 3159. In reaching its conclusion, the Court noted "[t]he marked distinction between the political 'message' of the armbands in *Tinker* and the sexual content of respondent's speech in this case." *Id.* at 680, 106 S.Ct. 3159. The Court recognized "that the constitutional rights of students in public schools are not automatically coextensive with the rights of adults in other settings." *Id.* at 682, 106 S.Ct. 3159. *Fraser* ultimately upheld the school's discipline of the student because of the school's need to teach students appropriate social behavior. *See Castorina v. Madison County Sch. Bd.*, 246 F.3d 536, 542 (6th Cir.2001) (citing *Fraser*, 478 U.S. at 683, 106 S.Ct. 3159). In making its decision, the Court drew a line between expression directed at a certain viewpoint and lewd and vulgar speech.

The court found that Coy created his website on his own time, his own computer, and not using any school resources. The issue to be tried: Did the school expel him for accessing an unauthorized website on his school computer (allowed) or because school officials did not like the crude, but not obscene, content of the website which no other student saw during the school period (not allowed).

Threats of violence often receive the least protection from federal courts. For example, a student's instant message prepared off campus and sent on private devices could still result in discipline. The instant messages went to 15 classmates over a three-week period, showed a pistol firing a bullet at a person's head and blood splatters. Under the head appeared the name of the student's English teacher. The court held the school did not violate the First Amendment by suspending the student. *Wisniewski v. Board of Educ. of Weedsport Cent. School Dist.*, 494 F.3d 34 (2d Cir. 2007).

The challenges to school discipline usually involve free speech, due process, or inequitable treatment. These result in expensive constitutional litigation under the First Amendment guarantee of free speech of the Fourteenth Amendment's extension of due process and equal protection to the states. Public schools can minimize the litigation risk. First, use neutral rules about content aimed at inappropriate material for children and disruption to the educational environment. Second, include a process in the disciplinary guide for serious offenses where the student and parents receive notice of the violations charged with some detail and an opportunity to present their side of the story before a final administrative decision. Third, review the individual cases at a higher level to make sure similar punishment results for similar conduct.

Private schools exercise broader control over their students and need not follow the prohibitions of the First and Fourteenth Amendments as they apply to governmental action. If, however, a nominally private entity's actual educational role is "entwined" with the government, then constitutional liability may result. *Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n*, 531 U.S. 288, 295–96, (2001) (Finding entwinement for private association that set athletic association that set rules for all high schools, public and private); *Lobiodice v. Trustees of Maine Central Inst.*, 296 F.3d 22 (1st Cir. 2002) (Finding no entwinement for private high school that accepted public school students under contract with school district). Private schools may also find themselves subject to federal litigation where their handbooks guarantee diversity and non-discrimination under 42 U.S.C. § 1981. If a private school receives direct federal funding, such as subsidized lunches under the National School Lunch Program, then Title VI of the Civil Rights Act applies. *Silva v. St. Anne Catholic School*, 595 F.Upp.2d 1171, 1181 (D. Kan. 2009). Claims against a private school for breach of contract, including breach of the covenant of good faith and fair dealing, can arise out of student discipline. *Southwell v. Univ. of Incarnate Word*, 974 S.W.2d 351, 356 (Tex. App. 1998).

LAPTOPS, TABLETS AND IPADS:

LEGAL CONCERNS

Forty years ago, students did not carry electronic devices around schools. Transistor radios, boom boxes, miniature televisions would all be confiscated and sent home as disruptive of the educational environment. This policy still exists as a required one for South Carolina schools. By requirement of the Department of Education, it is a Level I offense to possess an electronic communication device, including iPods, tablets and computers, at school in violation of school board policy. S.C. Code Ann. Regs. R. 43-279.

Despite this rule, today schools either require or encourage students to bring net capable laptops, iPads of tablet computers to school. These devices can access vast amounts of content far beyond the broadcast only electronic media available forty years ago. The proliferation, cost, ownership and related legal issues for these devices pose new and intricate problems for schools and school districts.

I. Funding and Ownership of Educational Electronic Devices: Legal Issues

A laptop, tablet computer or iPad in every pot costs much more than chicken today. When a school requires the use of such a device, what obligation does it have to pay for it? Is computer access part of a minimally adequate education today? If the answer is yes, then in South Carolina the Constitution mandates providing the

technology. S.C. Const. Art. XI, Sec. 3; *Abbeville Cnty. Sch. Dist. v. State*, 335 S.C. 58, 68, 515 S.E.2d 535, 540 (1999).

Allowing students to provide their own computers may be acceptable if the school provides for those who cannot. It may also be acceptable to allow parents with more means to provide their students more powerful computers than those provided by the school. In South Carolina, schools may use funds from the Public School Facilities Assistance Act for wiring, conduit, and powering of hardware installations for classroom computers and area networks, but not for computers themselves. S.C. Code Ann. § 59-144-30 (2017). Schools receive proceeds from the "Public Education: A Great Investment" automobile license plate sales for the purchase of computers. S.C. Code Ann. § 56-3-5010 (2017).

South Carolina began the venture into school provide laptops with grants donated by Blue Cross/Blue Shield in the One Laptop Per Child program. The State Department of Education developed a South Carolina Educational Technology Plan and required each district to develop its own technology development plan. In the 2016-2017 School Funding Manual, the Department allocates $35, $50 or $75 per pupil based on Average Daily Membership for implementing the plans. (**ATTACHMENT 8**, Manual Cover and pages 57-58, 114, 118-119). The three sections reprinted here show special funds from which districts may purchase computers.

Funding in South Carolina goes through an unusual process. The South Carolina K-12 School Technology Initiative made up of three government departments, the State Library, SCETV, and two private partners (AT&T and the SC Telecommunications and Broad Band Association) guides the expenditure of appropriated funds for software, hardware, and connectivity. http://sck12techinit.sc.gov/aboutus/Pages/InitiativePartners.aspx. The Initiative also provides easy to use forms and guidance for accessing E-Rate funds. The Initiatives Internet and WAN/LAN policies are attached as **ATTACHMENT 9**. The 2015-16 Initiative Report shows $24,988,067 in E-Rate funding disbursements. Each school and district must be sure to receive a portion of this. As of the last report year, students in 1193 schools out of 1248 can access the internet in 91% or more of the classrooms. 28.3% of all schools provided 91% or more students' 1:1 learning with a laptop.

It is apparent, despite the progress, that many schools not providing laptops to student do provide internet access. Section V below deals with an approach that may bring 1:1 sooner—allowing students to bring their own devices to school.

As schools hurry their transitions to 1-to-1, the law has not kept pace. And, as usual when technology has far outstripped legal theory, the best defense at the local level is robust school policies that have been considered and passed by the school board, particularly in regard to thorny issues like ownership, student safety,

and general usage in non-school environments. Districts should take into consideration how their funding structure will affect their legal responsibility and create their policies accordingly. Policies should take into account state and federal laws. Sample School Technology Policies can be found on the internet; for example: https://lasallian.info/.../2014/03/School-Staff-Technology-Policy.pdf.

II. Privacy – School Devices Allowed to Go Home and Searches/Control of BYOD

The starkest difference between BYOD (Bring Your Own Device) and 1-to-1 initiatives, at least legally speaking, is the issue of ownership, which is very important in search-and-seizure law (and the law in general). In this area, the constitutional protection offered by the Fourth Amendment serves to support schools with 1-to-1 programs, but leaves those who have gone BYOD open to more risk.

A public school student's protection against unreasonable search and seizure is less stringent in school than in the world at large. In *New Jersey v. T.L.O.*, 469 U.S. 325 (U.S. 1985), the U.S. Supreme Court general established that the Fourth Amendment of the United States Constitution provides school students with a limited expectation of privacy in the school setting and that searches based upon individualized suspicion must be reasonable. A school search requires "reasonableness under all the circumstances" (as opposed to probable cause). The analysis is a two-step process. (1) whether the search is justified at its inception (i.e., whether there are reasonable grounds for suspecting that the search will turn up

evidence that the student has violated or is violating either the law or the rules of the school) and (2) reasonable in terms of the scope of the search (i.e., whether the scope is reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction." *Id*. at 423-24; *See also Safford Unified Sch. Dist. No. 1 v. Redding*, 557 U.S. 364, 128 S.Ct. 2633 (2009). Other basic principles that can be taken from *T.L.O.* and applied more generally include:

- Public school officials do not merely exercise delegated parental authority conferred upon them by individual parents; rather school officials "act in furtherance of publicly mandated educational and disciplinary policies." *T.L.O.* at 417.
- Expectation of privacy includes a look at state and school district policies as well as how visible said policies are; for example, in a 2016 Iowa Supreme Court case, the Court paid at least some heed to the fact that the school posted its policy on the two main entry doors of the school building that all bags are subject to search. *State v. Lindsey*, 881 N.W.2d 411, 414 (Iowa 2016); *See also Iowa v. Benjegerdes*, No. 09-1230 at *8 (Iowa Ct. App. Sept. 8, 2011) (pointing out that what a person knowingly exposes to the public, even at home or in the office, is not protected by the Fourth Amendment).
- The Court is to balance against the student's interest in privacy the substantial interest of teachers and administrators in maintaining discipline and control in the classroom and on school grounds to achieve an environment conducive to all students learning a proper education. *Iowa v. Jones*, 666 N.W.2d 142, 150 (Iowa 2003).
- The trend is away from a rule-based search and seizure jurisprudence and toward a case-by-case method that will often turn on a careful and meticulous analysis of the facts of the case.
- When law enforcement is involved, full Fourth Amendment protections apply.

When schools own the devices being used in a 1-to-1 program, they arguable have an increased ability to monitor the activities on those devices and search the digital contents to investigate individualized suspicion of a disciplinary incident. Searching an iPad that a student is borrowing is like searching a locker (both are owned by the school), while searching a student-owned iPad is more like searching a purse that is clearly a student's private property. Thus, districts that have BYOD policies permitting student- or parent-owned devices in school could be more restricted in searching or seizing those devices after suspicious activities.

Courts have been more restrictive in how school officials may search such personally owned devices. For example, a recent court decision out of Kentucky prohibited searching cell phones for the general health and safety of the student without individualized suspicion of a discipline infraction. [CITE] However, such a decision would likely go the other way if the case concerned a school-owned laptop or mobile device.

While not involving a BYOD, the Fourth Circuit decided a case regarding school's rights to discipline for and monitor conduct occurring off-campus in *Kowlaski v. Berkeley County Schools*, 652 F.3d 565 (4th Cir. 2011). In that case, a student at Musselman High School in Berkeley County, West Virginia created a social media page on MySpace criticizing a fellow high school student as a slut and making fun of her. She also accused the fellow student of having herpes. The

student created the website from her home computer, away from campus, but invited many students to join the group.

School administrators concluded that the student created a "hate website" in violation of school policy against "harassment, bullying, and intimidation." *Id*. at 568-69. The court found that the schools may regulate off-campus behavior when the off-campus behavior creates a foreseeable risk of reaching school property and causing a substantial disruption to the work and discipline of the school. *Id*. at 571. The court determined that it was reasonably foreseeable that a "hate website" about a fellow student, inviting other students to be members, would be discussed in the school and disrupt classwork and create substantial disorder, thereby, colliding with the rights of others. Thus, it was appropriate of the school to suspend her for ten-days from school along with a 90-day social suspension.

The same sort of analysis can occur with activities on a BYOD. Even when used from home, if the BYOD is used in such a way that it could be foreseeably involved in the school's mission of education or seen by other students, or seen as injurious to administrators and teachers, then the school would have every right to investigate and, if appropriate, discipline the student.

The presence of BYOD devices can create a temptation for school officials. School officials cannot search a device, such as a cell phone, absent a connection to the suspected misconduct prompting the search. In a recent Virginia case, a school

official went to trial because of an unreasonable search of a cell phone in *Gallimore v. Henrico County School Bd.*, 38 F.Supp.3d 721 (E.D. Va. 2014). In that case, school officials received reports of a longhaired student meeting the plaintiff's description smoking marijuana on a bus. They searched various places on the student that could hide marijuana. They also searched his cell phone. The court found that part of the search objectively unreasonable because the cell phone could not hid marijuana. The fact that a device is present at the school does not open the door to a search without suspicion of a device related violation.

At issue is the concept of ownership (who actually purchased the device) rather than where the funds were obtained. Thus, even when parents pay usage fees for a device, if the school purchased it, the school retains a broader right to search the device unless specifically prohibited in the Acceptable Use Policy or other parental contract. (Think of the search restrictions in an apartment lease). Therefore, the question of who owns the device must be made clear, and districts should avoid any contracts or purchases that seek to provide joint ownership of the device. All school boards currently investigating a 1-to-1 deployment in their schools must make a very clear decision between school-owned and parent-owned devices.

III. Regulating Student Use of Devices: Risk and Responsibility

School districts are legally obligated to monitor to some extent how students use district-owned computers. They likely have the authority to investigate a student's personal mobile device in BYOD districts.

Schools may find themselves challenged on other legal grounds, such as failure to protect against civil wrongdoings committed by those with access to the devices. This could include the invocation of state and federal laws against bullying.

School districts should put into place strong parental notification policies to warn families they should not expect any privacy concerning the devices. They should require students to sign an agreement that warns them that everything they do on a school-issued device is subject to review by officials.[3]

School districts should use security filters (companies, software) to monitor cyberbullying, threats of violence, obscene language or messages indicating potential self-harm or criminal acts. In addressing security filters, there is always the need to balance security with too much security that interferes with usefulness of the device.

While not specifically delineated in this topic heading, as a practical matter, many of our cell phones contain much of the same capabilities and information as does our iPads and other mobile small computers. The United States Supreme Court has ruled generally on searches of cell phones: A cell phone itself does not pose any

[3] Black, Lisa (2014. *Student Computer Use Raises Privacy Questions*).

security threat as a weapon, and while it might possess potential evidence, once removed from the individual, the potential loss of evidence has been removed." *Riley v. California*, 134 S.Ct. 2473 (2014).

Health considerations could come to play. Therefore, policies should include and address avoiding "computer vision syndrome" or iStrain by providing a short break every 20 to 30 minutes.[4] Another health consideration is protection from Electromagnetic Radiation (EMR) that iPads, tablets and laptops emit.[5]

Insurance and security against potential theft and recovery for school-issued iPads and laptops, which have become a popular target for thieves, should be considered for schools developing and implementing technological device policies for students and staff.

IV. The Children's Internet Protection Act (CIPA) [Discussed Above]

A. CIPA Requirements

The Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection Act (NCIPA) went into effect on April 20, 2001. These laws place restrictions on then use of funding that is available through the Library Services and Technology Act, Title III of the Elementary and Secondary Education Act, ad on the Universal Service discount program, known as the E-rate (Public Law 106-554).

[4] (2016). *IStrain: Tablets and iPads Can Cause Eye Problems*. Retrieved from URL.
[5] *IPad Radiation: Ways to Protect Yourself*. Retrieved from https://www.defendershield.com/ipad-radiation-ways--protect-yourself/.

These restrictions take the form of requirements for Internet safety policies and technology which blocks or filters certain material from being accessed through the Internet. The deadline for compliance with NCIPA was July 1, 2002 for those libraries receiving 2002 E-rate discounts for Internet access or internal connections. The deadline for compliance with CIPA was July 1, 2004, following the Supreme Court ruling in 2003.

CIPA requires that K-12 schools and libraries use internet filters and implement other measures to protect children from harmful online content as a condition for federal funding. It was signed into law on December 21, 2000 and found to be constitutional by the United States Supreme Court on June 23, 2003.[6]

> Definition of "harmful to minors": Any picture, image, graphic image file, or other visual depiction that –(i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way, with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.[7]

B. An Example of Filtering

I suggested multiple filter products above that can assist a school with meeting this legal requirements above. Here is an example of how one works.

[6] Retrieved from http://www.ala.olg/advocacy/advleg/federallegislation/cipa
[7] Retrieved from http://fcc.gov/consumers/guides/childrens-internet-protection-act.

Providing students with a wholesome and healthy learning environment is an important facet of the productive teaching. With GoGuardian's Chromebook filtering, you never have to worry about how your students are using their Chromebooks in the classroom or at home. From blacklisting entire websites based on our CIPA compliant categories list to filtering individual YouTube videos by keyword or channel, GoGuardian offers complete filtering protection for every Chromebook in your fleet.

Determine which sites to blacklist or whitelist with our easy-to-use controls and redirect students to your own custom splash screen if thy attempt to access filtered content. Our proprietary content-based filtering software will also track and analyze every website that a student uses and flag sites that might contain questionable content, so you can go back later and decide for yourself if it should be blocked or not. If teachers and administrators require access to blacklisted sites or content, GoGuardian allows you to quickly setup temporary bypass passwords with specific time limits to allow specific users access to the blocked pages. Get peace of mind with the protection of GoGuardian's Chromebook filtering software and never worry again about what your students are accessing on the internet. Use our broad categories list to easily remain compliant with CIPA requirements. Filtering

is comprehensive: blacklist websites and filter YouTube videos by category, specific URL, and more.[8]

C. What Happens If Students Detect the Filter?

Filtering applications and hardware can only do so much. Schools implement them as an easy way to demonstrate CIPA compliance. Acceptable use polices also serve this purpose. Finally, live and remote monitoring of at school usage provides an added layer of protection.

Once a responsible school implements such a three-tier content control system, what consequences may occur if a student circumvents the content limitations? CIPA only requires a school to take appropriate protections. It is not a strict liability statute. CIPA stands in tension with the First Amendment.

The tension resulted in a preliminary injunction against school filtering of certain lesbian and gay related websites in *Parents, Families, and Friends of Lesbians and Gays, Inc. v. Camdenton R-III School District*, 853 F.Supp.2d 888 (W.D. Mo. 2012). The filtering software used by the school blocked may gay/lesbian support websites based upon the pornography search parameters used by the software. Students could petition to have site removed from the blocked list. The court found that the filtering blocked content that the First Amendment likely

[8] Retrieved from www.coguardian.com.

protected for access. The court also found the unblocking procedure amounted to an impermissible restriction on speech and led to fear of student stigmatization. As a result, the court granted a preliminary injunction requiring the school district to discontinue its internet-filter system and requiring any new system implemented could not discriminate against websites expressing a positive viewpoint toward LGBT individuals pending trial on the merits.

Congress attempts to make criminal the transmission of sexually explicit material to minors over the internet, the Communications Decency Act and the Child Online Protection Act, both failed for violating the First Amendment. *Reno v. ACLU*, 521 U.S. 844, 870-71 (1997); *Ashcroft v. ACLU*, 542 U.S. 656 (2004). Congress shifted its focus to preventing the receipt of sexually explicit material with CIPA.

CIPA does not provide for a private cause of action or school liability other than loss of eRate funding for failure to comply. Parents may sue a school, however, for harm to students resulting from negligence or negligent supervision. Exposure to sexually explicit material at school in violation of school policy may result in liability if the school's policies, supervision and enforcement are negligent and a student suffers some injury as a result.

V. The "Bring Your Own Device" Solution and Unique Legal Issues

What happens if the school allows a student to use his/her own devices? Student/parent owned devices present unique legal issues. The school MUST get student/parent permission to apply filtering software to comply with CIPA and NCIPA. The school must require that student and parents/guardians sign a consent to use and consent to access form for the equipment agreeing to follow acceptable use and to allow school officials to access and monitor the device.

The Bring Your Own Device (BYOD) solution suffers from obvious fairness issues. Wealthy parents or those with access to work technology discount programs may provide much better equipment to their students while other student may have none. Handling this disparity will tax school policy making and monitoring. Advantages to BYOD:

- Immediate technology integration;
- Concentrate school funds on students in need;
- Opportunities for personalized learning;
- Students know how to operate these devices without school instruction;
- Students unlikely to forget them at home;
- Students may be more likely to continue work/learning after hours; Disadvantages;
- Curriculum may not be universal across platforms used;
- May tax bandwidth and infrastructure, cause support issues;
- Some devices ill equipped for classroom use;
- Create legal ownership and search/seizure issues;
- Increases possibility of cheating, especially in tech savvy households; and
- May make student more likely to be distracted than on a school issued limited machine.

In order to address these problems, schools must develop both technology and use/access policies and contracts about what devices students may bring to school and how students may use their private devices. As stated above, a contractual agreement should allow school personnel to access and student devices used in the program. In most states, a minor cannot own property so the parent/guardian must be part of the agreement.

The school must mandate more than filtering software. Data protection, encryption, and network protection must come on each device. The school can require the family or provide software. The school faces the same problems that an employer does who allows employees to use private devices. The school must insure proper software, hardware and other protective devices or its entire network may be at risk. The contract between the school and parents must clearly set out what the school owns (data, provided content, provided applications etc.) and what the family owns.

Clarity Innovations publishes an introductory tool kit on BYOD found at https://www.k12blueprint.com/toolkits/byod that you may find useful.

BYOD solutions pose another legal issue. Like other government agencies, public schools must abide by public records laws. The Freedom of Information Act (FOIA) in South Carolina applies to school districts, school boards, and even school administrations. The definition of a public body subject to FOIA specifically

includes school districts. S.C. Code Ann. § 30-4-20(a) (2017); *New York Times Co. v. Spartanburg County School Dist. No. 7*, 374 S.C. 307, 649 S.E.2d 28 (2007). Any person may inspect or copy any public record of a public body. S.C. Code Ann. § 30-4-30. Non-school related information on a BYOD does not fit the definitions of FOIA. FOIA also exempts personal information that would invade privacy. S.C. Code Ann. § 30-4-40(2).

Citizens may argue that information related to the education services of the school and school policies residing on a privately owned but consensually used BYOD constitutes a public record subject to FOIA. At first blush, it would appear that privately owned data and machines do not fall within the scope of FOIA. The Supreme Court of South Carolina found, however, that FOIA did not violate the First Amendment to the constitution if applied to a private, non-profit entity should discovery show that entity to be a public body in *Disabato v. South Carolina Assoc. of School Administrators*, 404 S.C. 433, 746 S.E.2d 329 (2013). Private actors entwined in school district business may be subject to FOIA.

A cautionary note on the personally identifiable information of students—publishing it, selling it or using it for non-school purposes may lead to liability. Court and legislature take privacy and identity theft concerns very seriously as do federal regulators. North Carolina has specific statutes protecting student

information in public and private schools. N.C. Gen. Stat. Ann. §§ 115C-401.1 and 115C-566.1.

CONCLUSION

Technology and the internet will provide new educational resources and expanded access to more and more up-to-date resources for educators and students. Legal and practical issues will emerge from the expansion of technology and web access in schools and for use by students at home.

We hope these materials provide a good starting point for analysis and thoughtful policy making for this exciting and expanding frontier in education.

Please feel free to call me or email me with follow up questions.

ATTACHMENT 1

RICHLAND COUNTY SCHOOL DISTRICT ONE

digital

LEARNING ENVIRONMENT

2015-2016 Digital Learning Environment (DLE) Technology Handbook For Students and Parents

---

We are Richland One, a leader in transforming lives through education, empowering all students to achieve their potential and dreams.

Revised August 21, 2015

Richland One
South Carolina's Capital Schools

Board of School Commissioners

Cheryl Harris, *Chairwoman*
Mr. Vince Ford, *Vice Chairman*
Mrs. Pamela Adams, *Secretary-Treasurer*
Mr. Dwayne Smiling, *Parliamentarian*
Mr. Jamie L. Devine
Mrs. Beatrice King
Mr. Aaron Bishop

Superintendent

Dr. Craig Witherspoon

VISION

Richland School District One, in collaboration with an engaged community, is committed to ensuring that each learner achieves his/her potential in a safe, caring, academically challenging and diverse learning environment that will develop productive citizens for a changing world.

MISSION

We are Richland One, a leader in transforming lives through education, empowering all students to achieve their potential and dreams.

1616 Richland Street
Columbia, South Carolina 29201
www.richlandone.org

Richland School District One

South Carolina's Capital Schools

Office of the Superintendent

August 2015

Dear Students, Parents and Guardians:

We live in a digital world. Technology is part of our daily lives. In Richland One, teachers and students have been using technology in the classroom for many years and we have a wide array of technology resources. Our Digital Learning Environment (DLE) initiative will expand the integration of technology into the curriculum to ensure that we prepare our students for college and careers.

The use of technology enhances teaching and learning, boosts student engagement and empowers teachers to differentiate, individualize and personalize instruction. The 1:1 (one-to-one) component of DLE will provide our students with powerful technology tools to use to enhance their ability to think critically and creatively, work independently and collaboratively, communicate effectively and solve problems.

During the Fall of 2015, laptop computers will be distributed to all middle and high school students. Devices will be distributed to students in grades 3-5 in January 2016. At the conclusion of the distribution, all students in grades 3-12 will have personal computing devices. Students in pre-kindergarten through second grade will have access to school and classroom sets of computing devices.

It is important to understand that the focus of DLE is not on the devices but on using technology to transform teaching and learning in Richland One. Teachers will be able to create individualized instruction that is truly student-centered. Students will become the producers and evaluators of knowledge, not just consumers. Students also will collaborate with others to engage in authentic, real-world tasks. Most importantly, they will develop the skills they need to compete in today's digital world.

Please take time to review the information in this handbook carefully. If you have questions or need additional information, please contact your school.

Sincerely,

Craig Witherspoon, Ed.D
Superintendent

1616 Richland Street • Columbia, South Carolina • 803.231.7500 • Fax 803.231.7502 • www.richlandone.org

Receiving/Turning in Your Laptop

Distribution of Laptops

- Schools will conduct orientations each year for parents/guardians and students. Parents/guardians and students must attend the orientation and parents/guardians must sign the Parent Consent Form and pay the Mandatory Protection Plan.
- Laptops will be distributed each year during each school's laptop distribution schedule.
- Students will sign the Acceptable Use Policy and log into the district's network.
- Students must bring their student ID to the laptop distribution.
- Students will be issued a laptop, power cord, computer sleeve and backpack. Only one backpack will be issued; it becomes the student's property and does not need to be returned.

Turning in Laptops

- Students transferring from a school or leaving Richland County School District One during the school year must return the laptop (including power cords and any other district- or school-issued accessories) before leaving the school. Students will keep the backpack.
- Students transferring to another school in Richland One will not take the laptop (or accessories) with them. They will return it to their departing school and will receive a laptop at their new school.
- If a student does not return his/her laptop upon leaving the district, the student will be subject to criminal prosecution or civil liability. The student also will be required to pay the replacement cost for a new laptop.
- If a student returns his/her laptop device damaged, costs for replacement or repairs are the responsibility of the student/parent/guardian. The district will charge the student/parent/guardian the cost of needed repairs, not to exceed the replacement cost of the laptop.

Identification of Laptops

- Laptops will have a district asset tag with Dell Service Tag number and Fixed Asset Tag number.
- Follett's **Destiny Asset Manager** will be used to assign laptops to students.
- Laptops will be scanned in/out using a handheld scanner and the **Follett's Destiny Asset Manager Software.**

Caring for Your Laptop

- The laptop is district property. All students will follow these guidelines and the Richland One Acceptable Use Policy.
- Students are responsible for the general care of their laptops.
- Students must immediately report any damage to their laptops to the school.
- Students/parents/guardians must report stolen laptops to law enforcement and the school within 24 hours of discovering it missing.

General Precautions

- Keep food and liquids away from your laptop. Don't eat over your laptop; the crumbs can fall between the keys and provide an invitation to small bugs or damage the circuitry.
- Always have clean hands when using your laptop.
- Protect the screen. When you shut your laptop, make sure there are no small items, such as a pencil or small earphones, on the keyboard. These can damage the display screen if the laptop is shut on them; the screen will scratch if the item is rough. Close the lid gently, holding it in the middle. Closing the lid using only one side causes pressure on that hinge, and over time can cause it to bend and snap.
- Hold and lift the computer by its base, not by its screen. If you lift it by the screen alone, you could damage the display or the hinges attaching the display to the base. The display is also easily scratched or damaged by direct pressure – avoid placing pressure on it.
- Don't pull on the power cord. Tugging your power cord out from the power socket rather than pulling directly on the plug can cause the cord to break off from the plug or damage the power socket. Also, if the power cord is near your feet, avoid kicking it accidentally. Refrain from bumping into the plug at all because it could loosen it and eventually break.
- Don't roll your chair over the computer cord. Stick the cord onto your desk with tape or a special computer cord tie which can easily be undone when you've finished using the laptop. Always try to keep the cord away from the floor and your legs.
- Be sure to plug accessory devices into their proper slots. Always look at the symbols on the laptop carefully before inserting devices. Jamming a phone line into an Ethernet port or vice versa could damage the sockets, making it impossible to use them again. It is very important to observe this step.
- Insert drives into their slots carefully and at the correct angle. Pushing the drive too forcefully into its slot could jam it.
- Don't leave your laptop in a car. Not only do the insides of cars experience large temperature swings that could damage a laptop, but a laptop (or laptop bag) is an inviting target for a smash-and-grab thief.
- Avoid placing heavy materials, such as books, on top of your laptop. This can push the screen into the keyboard, and will eventually damage it.
- Use the laptop on a flat, clean surface. This prevents damage to the laptop. This can be hard to do, particularly if you are outside with your laptop, but if there is a flat surface available, put your laptop on it.
- Do not share login information.
- Do not leave your laptop unattended unless it is stored securely behind a lock.

http://www.wikihow.com/Take-Good-Care-of-Your-Laptop-Computer

Carrying Laptops

- The district provides students with a protective computer sleeve for their laptop.
- Students will receive a district provided backpack.
- Use the district provided computer sleeve and backpack (or personal backpack). This will help avoid scratching, squeezing or potentially dropping it.

Using Your Laptop

- Laptops are intended to be used at school each day.
- Students are responsible for bringing their laptop to all classes, fully charged.
- In addition to teacher expectations for device use, students may access school messages, announcements, calendars and schedules using their laptop.

Laptops Left at Home

- Students who leave their laptop at home are still responsible for completing their daily coursework.
- Repeated offenses may result in disciplinary action.

Laptops Undergoing Repair

- Schools may issue a loaner laptop to a student while his/her laptop is being repaired.
- A student may not receive a loaner laptop immediately. There may be a delay depending upon availability.
- Students are still responsible for completing their daily coursework.

Charging Your Laptop's Battery

- Laptops must be brought to school each day fully charged. Students must charge their laptops at home each evening before school the next day.
- Repeat violations of not charging the battery for the school day may result in students being required to "check out" their laptop daily from the school.

Printing

- Students can print from their laptops.
- Schools will identify printers students may use; these printers will be mapped to student laptops.

Home Internet Access

- Students may establish Wi-Fi connections with their laptop outside of school.
- Students can use their laptop wherever access is available.

Camera Use

- The laptop has a front-facing camera and video capabilities.
- The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents and students over 18 years of age certain rights with respect to students' educational records, including photographs. For this reason, students must obtain permission to publish or make publicly available a photograph or video of any school-related activity.

Unauthorized recordings are subject to disciplinary action in accordance with the district's Acceptable Use Policy.

- Richland County School District One retains the right to any recording and/or publishing of any student or staff member's work or image.

Student Responsibilities for Laptop Care

- Each student is responsible for maintaining his/her laptop. Laptop batteries must be charged and ready for school daily.
- Only labels or stickers approved by Richland County School District One may be applied to the laptop.
- Backpacks will not be returned to the district. However, students are expected to keep them clean and in good repair to protect the laptop.
- Malfunctioning or damaged laptops must be reported to the school's Student Support Center. The district will be responsible for repairing laptops.
- Students are responsible for any and all damage to their laptop beyond daily wear and tear.
- Stolen or lost laptops must be reported within 24 hours to law enforcement and the school.

Managing Your Files and Saving Your Work

Saving to Your "F Drive"

- Each student is provided file storage space - "F Drive." Students are strongly encouraged to store all files on their F Drive because it is backed up each night.
- Students have permissions set to allow them to store files on the laptop hard drive. Students are strongly encouraged to transfer these files to their F Drive when at school to allow back up.
- Students will be provided "cloud-based" storage for their school files and work.
- Laptop malfunctions are not an acceptable excuse for failure to submit work.

Network Connectivity

- Do not share your login information with anyone.
- Richland County School District One makes no assurance that the network will be operational at all times.
- In the rare instance that the network may not be operational, the district will not be responsible for lost or missing data.

Software/Applications Installed on Laptops

Originally Installed Applications

- All applications originally installed by the district on each laptop must remain on the laptop in usable condition and readily accessible at all times.
- You may not remove these required applications and staff will periodically check laptops to ensure that students have not removed them. The school also may add other applications periodically.
- Some licenses for applications require that the application be deleted from the laptop at the completion of a course. If this applies to an application used by a student, technology staff will re-sync the devices of the students in that course.

Additional Applications

- Richland One syncs laptops so that the devices contain the necessary applications for schoolwork.
- Students will not be permitted to load additional software/applications on their laptops, in accordance with the district's Acceptable Use Policy. You can read the entire Acceptable Use Policy in Appendix A.

Inspection

- Staff will randomly select students and ask them to provide their laptop for inspection.

Procedure for Reloading Applications

- If technical difficulties occur or unauthorized applications are discovered, technology staff will re-sync the laptop.
- The school does not accept responsibility for the loss of applications or documents deleted due to a re-sync.

Application Upgrades

- The district will distribute upgraded versions of licensed applications from time to time through network processes or manually by a technician.

District Responsibilities

- The school provides Internet and e-mail access to students.
- School staff will help students conduct research and ensure student compliance with the district's Acceptable Use Policy *(see Appendix A)*.
- Filtering/blocking of inappropriate Internet materials is done at the district level; filtering/blocking also will occur when laptops are used outside the district.
- The district reserves the right to investigate any inappropriate use of resources and to review, monitor and restrict information stored on or transmitted via district-owned equipment and resources.
- The teacher is still the classroom manger; if the student is off task, the teacher has the ability to close and/or take a student's laptop.

Teacher Responsibilities

- Design instructional activities that make appropriate use of technology and digital resources
- Monitor and supervise student use of devices and direct their involvement
- Adhere to and provide instruction on the district's AUP

Student Responsibilities

- Students will abide by the district's Acceptable Use Policy *(see Appendix A)* and:
    - Contact an administrator about any security issue they encounter.
    - Monitor all activity on their personal account(s).
    - Always shut down and secure their laptop after use to protect their work and information.
    - Report e-mail containing inappropriate or abusive language or questionable subject matter to a teacher or administrator at school.
    - Return their laptop to the issuing school on the date they withdraw from school or transfer to another school. (This also applies to seniors who leave school mid-year or who graduate.)
    - Downloading/installing unauthorized applications, games or software is prohibited

Parent/Guardian Responsibilities

- Talk to your students about the values and standards you expect your children to follow as they use the Internet just as you talk to them about their use of all other media information sources, such as television, telephone, movies, radio, etc.
- All district-issued laptops contain a filter for use at home. Parents are encouraged to monitor student activity at home, especially Internet access.
- Report any vandalism or theft to law enforcement and the school with 24 hours of discovery.

Laptop Damage, Theft or Loss

Terms of the Mandatory Protection Plan (MPP)

- Parents/guardians are required to participate in the MPP.
- The full-year MPP cost is $30.00 per student, per school year and is non-returnable.
    - Payments may be made in installments if desired by parents/guardians
    - School-level staff will receive and receipt all MPP payments
    - At the time of distribution, if a payment has not been received, the school will issue a debt slip, allowing the student to receive a device. There must be a signed Parent Consent Form and signed Student Agreement on file to complete this process.
    - If the laptop is repaired or replaced the MPP must be paid in full before the laptop is returned to the student
- The MPP covers parts and repair for system-related issues or failures from normal use. It does not cover intentional damage or damage associated with misuse of the laptop.
- The MPP also covers:
    - One device replacement per school year in the event of theft, loss or accidental damage and/or;
    - One screen replacement due to accidental damage and/or;
    - Any additional replacement or repair will cost the student/parent/guardian the full cost of repair or the full market value of a device.
        - 1st year – 100%
        - 2nd year – 75%
        - 3rd year – 50%
        - 4th year – 25%
    - Power cords or other accessories are not covered by the MPP; student/parent/guardian are responsible for the full cost of replacement
    - In the event a laptop is stolen or lost, the student/parent/guardian must report the theft or loss to the school and file a police report within 24 hours. If the loss or theft is not reported within 24 hours, the student/parent/guardian may be liable for the cost of replacing the laptop.
    - Deductibles will be charged for each incident as described below:

Deductible	Cost
1st	$0
2nd	$20
3rd	$50
4th	Full cost of repair or replacement

Title

- Legal title to the laptop is with the district and shall at all times remain with the district.
- The right of possession and use is limited to and conditioned on full and complete compliance with the MPP and AUP.
- The student is responsible at all times for the laptop's appropriate care and use.

Repossession

- Richland County School District One reserves the right to repossess any laptop for failure to comply with all terms of the MPP and/or the AUP.

Liability

- Richland One reserves the right to demand return of the laptop at any time. The MPP is good for one school year (from the first day of school until the first day of school in next school year), unless the agreement is terminated earlier.
- Failure to return the laptop to the issuing school before departure from the district may result in criminal charges brought against the student and/or the person in possession of the laptop.

In the event of loss

- In the event a laptop is lost, the student/parent/guardian must report the loss to the school and file a police report within 24 hours.

In the event of theft or vandalism at school

- In the event a laptop is stolen, vandalized, etc., the student or parent/guardian must report the theft or loss to the school and file a police report within 24 hours.
- The student/parent/guardian must file a police report with the school resource officer (SRO) when incidents of loss, theft, vandalism, etc. occur on campus.

In the event of theft or vandalism off school and or of town

- If an incident occurs out of town or out of state, the student/parent/guardian must file a police report with the law enforcement agency covering that town or state within 24 hours and provide a copy of the completed police report to the school.

Daily Checkout/Use of Laptops

Parents/Guardians Do Not Approve Students Taking Laptop Home

- If parents/guardians do not approve students taking the laptop home, the laptop will remain at the school.
- Students will pick up the laptop in the morning, use it during the school day and return it before departing for home.
- Schools will develop procedures for daily use/checkout.
- If students violate the AUP or any part of this handbook, their use of the laptop may be restricted to use at school only.

Appendix A - Richland County School District One Acceptable Use Policy

Policy IJNDB Acceptable Use of Information Systems
Issued 03/09

Purpose: To establish the board's vision for access and use of the district's information system.

Richland County School District One will provide board members, employees and students with access to the district's electronic communication system which includes network, Internet and e-mail access. The principle purpose of this system is for the education of students and professional use by staff. This purpose includes use of the system for classroom, work-related, professional and career development activities.

The superintendent will continue to develop and implement procedures for the technical operation and management of the system, to facilitate its effective integration into the instructional programs at the schools and to address any related functions to ensure the purposes of the system are recognized. Appropriate forms and guidelines will support this policy and are published as separate documents which carry all the force of the board policy.

All uses of the electronic communication system by board members, employees and students are not confidential and may be monitored at any time by designated staff.

Richland County School District One is not liable for inappropriate use of the district's electronic communication system, copyright violations, user mistakes or negligence or costs incurred by users. The district is not responsible for the validity of any information found on the Internet or other external data systems.

This policy, administrative rule and its supporting forms may be accessed via the Internet from the district's website.

Adopted 5/23/00; Revised 6/6/05, 3/10/09, 8/25/15

Legal references:

Federal law:

47 U.S.C. Section 254(h) - Children's Internet Protection Act.

The Digital Millennium Copyright Act of 1998, Section 512 - Limitations on liability relating to material online.

S.C. Code of Laws, 1976, as amended:

Section 10-1-205 - Computers in public libraries; regulation of Internet access.

Section 16-3-850 - Encountering child pornography while processing film or working on a computer.

Section 16-15-305 - Disseminating, procuring or promoting obscenity unlawful; definitions; penalties; obscene material designated contraband.

Policy IJNDB-R Acceptable Use of Information Systems
Issued 03/09

STATEMENT OF INTENT
Richland School District One provides an electronic network and Internet access to enhance your educational experiences. Access to electronic and web-based resources is available through classrooms, media centers, computer labs and home computers. Through active learning experiences, students are expected to develop appropriate information literacy skills to ensure effective use of the wide variety of tools available through the network. As a network user, you are required to participate in Acceptable Use Policy training and always follow these important practices.

E-mail accounts are available to students in grades 3-12 unless denied by parents/guardians. All e-mail messages and electronic files created or stored using district resources are property of the district. Policy IJNDB and this Administrative Rule fully outline the district's intent, expectations, users' responsibilities and penalties regarding the network and its associated components.

Compliance with this policy is mandatory and includes access and use of the district information system and all peripheral devices for printing, storing, archiving and duplicating information regardless of location.

Use of the system carries a limited privacy expectation for all activities and files by all users. Parents have the right at any time to request in writing to see the contents of student e-mail and stored files.

Be aware that personal files are discoverable under the State of South Carolina's Freedom of Information Act. Richland One has the right to place restrictions on the material accessed or posted through the system.

Access to and use of the district system is provided as a privilege, not a right. All violations of the Acceptable Use Policy and its associated Administrative Rule will be investigated and will result in one or more of the following consequences:

- Limiting, suspending or canceling use and access to the system
- Confiscation of personal devices
- Applying penalties in accordance with the *Discipline Code*
- Levying fines and payments for damages, repairs and hardware replacement
- Application of civil or criminal liability under other applicable laws
- Expulsion

ACCEPTABLE USES

- Student e-mail is limited to educational purposes. The term "educational purposes" includes classroom activities, career development, completing applications to colleges and universities, and other high-quality discovery activities as determined by the school district. Non-classroom activities, such as using e-mail to communicate with prospective colleges or universities, will at no time take precedence over classwork.
- For school-related business, you may download text and other non-executable files attached to e-mail messages. You are encouraged, where possible, to download large files during off-peak hours.
- You will check your e-mail frequently, delete unwanted messages promptly and stay within your e-mail quota. Be aware that e-mail may be deleted by system administrators at any time.
- You can subscribe only to high-quality discussion group mail lists at the direction of your teacher that are relevant to your education or career development.
- Your right to free speech, as set forth in the "Discipline Code" applies also to using e-mail and any other form of online communication. This student e-mail system is considered a limited forum, similar to the school newspaper, and therefore the district may restrict your speech.
- You will immediately notify a teacher or the system administrator if you have identified a possible security problem. Do not actively seek security problems but immediately report any potential issues that are found.

CONDITIONS OF USE

- The Family Education Rights and Privacy Act (FERPA) is a federal law that affords parents and students over 18 years of age certain rights with respect to the student's educational records.
- Richland County School District One retains the right to any recording and/or publishing of any student or staff member's work or image.
- Employee and student use of district communication and computer systems shall be filtered for appropriate usage and content. Filtering shall be provided for all internet enabled computers used by students, patrons and staff. Filtering should be disabled only for bona fide research or other lawful purposes.
- Downloading/installing unauthorized applications, games or software is prohibited. This includes, not limited to proxy server software.
- If technical difficulties occur or unauthorized applications are discovered, technical staff will reimage the laptop. The school does not accept responsibility for the loss of applications or documents deleted due to a reimage.

PROHIBITED USES

Students who violate the terms of the Acceptable Use Policy or otherwise misuse the technology resources provided, will be subjected to disciplinary action for a Level 2 Offense, as outlined in Section IV-I (Other Unlawful Activities) of the Richland One *Discipline Code*. Specific prohibitions include:

- Using e-mail account for commercial purposes or political activities
- Using social media inappropriately including bullying, posting personal information, posting information that could cause a disruption or reflect negatively on the school district
- Posting chain letters or engaging in spamming
- Using e-mail for personal use, with the exception of contacting a parent/guardian for school-related or emergency purposes
- Posting personal contact information about yourself or other people (name, address, telephone)
- Agreeing to meet with someone you have met online without parent's/guardian's approval
- Promptly disclosing to your teacher or other school officials any message received that is inappropriate
- Not attempting to gain unauthorized access to the system or performing unauthorized functions
- Accessing another person's files
- Deliberately attempting to disrupt the information system, destroying data, or spreading viruses
- Engaging in other illegal acts such as arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, threatening the safety of a person in an intention or joking manner
- Sharing account information, IDs, and passwords with others
- Not downloading or run executable files attached to e-mail or using portable data storage devices which contain viruses or in any other way knowingly spread computer viruses
- Using inappropriate language in public and private messages, stored files and materials on web pages
- Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or gang-related language or symbols
- Posting information that could damage or cause a disruption to the system
- Engaging in personal attacks or harassing another person
- Knowingly or recklessly posting false or defamatory information about another person or organization
- Accessing material that is profane, obscene, pornographic or sexually explicit, that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature)
- Reposting a message that was sent to you privately without the author's permission or other activity of the information system that causes a disruption.

PARENTAL NOTIFICATION AND RESPONSIBILITY

- The district will notify parents/guardians about the district digital environment, related safety issues and issues governing its internet through a general letter to all parents. Parental permission is not required for use of the internet, but parents will be notified that they have the right to file a Parent/Guardian Denial Form available from the school principal if they do not want their children to have access to the digital learning environment. A parent/guardian may request in writing alternative activities for their child(ren) that do not require internet access with the understanding that such a request limits student opportunity and academic involvement.
- If a child has been denied access to the internet by a parent/guardian, then the parent/guardian must communicate to the child that he/she is to be restricted and is to discuss alternative activities with the teacher when instruction requires use of the internet. It is incumbent upon the student to respect his/her parent's/guardian's decision regarding denial to internet resources.
- A parent/guardian may request in writing at any time the right to see the contents of the child(ren)'s individual e-mail and stored files. Parents/guardians have the right to request in writing the termination of their child(ren)'s individual account at any time.

- The district's Acceptable Use Policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not possible for the district to monitor and enforce a wide range of social values in student use of the Internet. Further, the district recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The district will encourage parents/guardians to specify to their child(ren) what material is and is not acceptable for their child(

PROCEDURES

District Responsibilities

- The Superintendent or his/her designee will serve as the administrator to oversee the district system.
- The building principal or district department head or his/her designee will serve as local administrator for the district system.
- The principal/department head may designate a staff member (at the school level, preferably the Information Technology Specialist), to act as coordinator of system use and management.
- The building/department level coordinator will submit all e-mail account applications to the IT Helpdesk and will maintain a file of e-mail applications.
- The principal/department head will approve building/department level activities, and will ensure that users receive proper training in the use of the system and the requirements of this policy.
- The principal will establish a system to ensure adequate supervision and training of students using the system and will maintain a file of Student E-mail Use Agreements.
- The Executive Director of Information Technology will establish a process for setting up employee network and e-mail accounts, set quotas for file storage on the system, and

establish file retention and backup schedules, a district virus protection process, and an Internet filtering system that meets Children's Internet Protection Act (CIPA) requirements. He/she will oversee the administration and maintenance of the district's network infrastructure and operations, and the district's management information system).

- The Director of Communications will oversee the design and maintenance of the district web presence. The Technology Leadership Committee will coordinate the selection and purchase of software, hardware and electronic resources.
- The Director of Instructional Technology Services will collect and report usage statistics for these resources. He/she will manage the technology staff development of district employees, school web administrators and teachers in the use of the schools' web-based communication system and in the use of district online resources.
- The Director of Professional Development will maintain and administer online certification and professional development data.

Due Process for Students

- The district will involve law enforcement should illegal activities take place.
- Student users who mistakenly access inappropriate information or images should immediately report this to a school staff member. This will initiate proceedings to have sites reviewed.
- The district will provide students and parents/guardians with guidelines for student safety while using the district information system.
- In the event there is an allegation that a student has violated the district Acceptable Use Policy, the student will be provided with a written notice of the alleged violation and an opportunity to present an explanation to be heard in the manner set forth in the Richland County School District One *Discipline Code.*

DISCLAIMER OF LIABILITY

- The district makes no warranties of any kind, either expressed or implied, that the functions of the services provided by or through the district system will be error-free or without defect. The district will not be liable for the users' inappropriate use of the district's electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The district will not be responsible for ensuring the accuracy or usability of any information found on the Internet.

DISTRICT WEB PAGES

- The district's website is www.richlandone.org. The Office of Communications will maintain the home page.
- Departments will establish web pages that present information about department activities and resources based on district specifications.
- Schools will establish web pages that present information about the school and class activities based on district specifications. The building principal will designate an individual to be responsible for coordinating and managing the school website, which includes establishment and posting of material to the district web page.

- Teachers will establish class web pages that present information about the school and class activities based on district minimum specifications.
- Student web pages must include the following notice: "This is a student web page. Opinions expressed on this page will not be attributed to the district."
- With the approval of the building principal, extracurricular organizations may post their information as part of the school web page. This information must relate specifically to the organization's activities and be submitted to the faculty sponsor before posting. Organization web pages must include the following notice: "This is a student extracurricular organization web page. Opinions expressed on this page will not be attributed to the district."
- Commercial purposes are defined as offering or providing goods or services or purchasing goods or services for personal use.
- Internet: Upon signing the district Internet Use Agreement, all district employees, board members, and students will have access to the World Wide Web through the district's networked computers. The Internet is considered an important research tool for students and employees. Parents may specifically request that their child(ren) not be provided access. However, it should be understood that all activities are curriculum driven and that to deny access is to limit the student's ability to participate in instructional opportunities.
- Harassment. Persistently acting in a manner that distresses or annoys another person.
- Employee Intranet: All board members and district employees will have access to additional resources through the district Local Area Network (LAN) and Wide Area Network (WAN). Access to resources that include confidential information will be password protected, and the department responsible for the administration of the resource will assign access rights.
- School Intranets: Students and school employees will have access to additional resources through the school Local Area Networks (LANs). Access to resources that include confidential information will be password protected, and the department responsible for the administration of the resource will assign access rights.
- Student E-mail Accounts: Parents may specifically request that their child(ren) not be provided access. However, it should be understood that all activities are curriculum driven and that to deny access is to limit the student's ability to participate in instructional opportunities.
- District Employee E-mail Accounts: All employees must agree to abide by the district's employee e-mail use agreement in order to initialize the account and to renew that agreement annually.
- Guest E-mail Accounts. Guests may receive temporary individual e-mail accounts with the approval of a district administrator if there is a specific, district-related purpose requiring such access. Administrators must submit the name of a guest request to the IT Help Desk. Guest users must agree to abide by the district's employee e-mail use agreement in order to initialize the account and to renew that agreement annually. Use of the system by a guest must be specifically limited to the district-related purpose. A parental signature is required if the guest is a minor.
- Spamming: Spamming is sending an unnecessary message to a large number of people.

ACCEPTABLE USE POLICY GUIDELINES FOR STUDENTS
(date)

Richland School District One provides an electronic network and Internet access to enhance your educational experiences. Access to electronic and web-based resources is available through classrooms, media centers, computer labs, district issued devices and home computers. Through active learning experiences, you are expected to develop appropriate information literacy skills to ensure effective use of the wide variety of tools available through the network. As a network user, you are required to participate in Acceptable Use Policy training and always follow these important practices. E-mail accounts are available to students in grades 3-12 unless denied by parents/guardians. All e-mail messages and electronic files created or stored using district resources are property of the district. Policy IJNDB, its Administrative Rule and related policies including Copyright Compliance and BYOD (Bring Your Own Device), fully outline the district's intent, expectations, users' responsibilities and penalties regarding the network and its associated components.

STUDENT AGREEMENT
In order to take full advantage of these resources, I will:

- Read and abide by all sections of the Richland One Acceptable Use Policy and Administrative Rule Guidelines.
- Use the system for educational purposes only including classrooms activities, career development, college applications and other activities as determined by the district.
- Protect myself by never posting personal contact information or account information (passwords/logins) about myself or others.
- Respect the district network and not attempt to gain unauthorized access to the network, website, Internet or online resources.
- Refrain from destruction and vandalism of the network system and its hardware.
- Notify teachers or administrators of any inappropriate e-mail messages or possible system security problems.
- Refrain from inappropriate, obscene, profane, vulgar, rude, inflammatory, threatening, disrespectful or gang-related language or symbols.
- Use district owned and identified resources and not download or install unauthorized software or executable files, including, but not limited to proxy server software with the intent of circumventing the district filter
- Use network and e-mail access responsibly, understanding that it is a privilege and all violations will result in disciplinary measures as outlined in the Disciple Code.
- Refrain from sharing account information including user name and passwords

PENALTIES FOR IMPROPER USE
Students who violate the terms of the Acceptable Use Policy or otherwise misuse the technology resources provided, will be subjected to disciplinary action for a Level 2 Offense, as outlined in Section IV-I (Other Unlawful Activities) of the Richland One *Discipline Code*.
I understand each of these Acceptable Use Policy guidelines and agree to abide by them and all components of the policy and Administrative Rule.

Student's Name (Print) _____

Student's Signature _____ Date _____

Parent Form for Denial of Student Use of Internet and E-mail Resources

Acceptable Use Policy of Information Systems (IJNDB)-Administrative Rule

(To be filled in by the school)

The involved parent or guardian must sign this form before Internet and E-mail use can be denied to a student in Richland County School District One. The form should be submitted to the principal. The site-based coordinator will file the form and provide a copy to the parent. The site-based coordinator will furnish teachers with a list of students who are being denied access to the Internet. The parent through written notification to the school principal may retract the denial. The principal will notify the site-based coordinator of any retraction of denial.

Parent's Name: _____ **Date:**_____

Student's Name: _____

Homeroom Teacher: _____

Principal and School: _____

I have read the letter concerning the use of the Internet and E-mail in Richland County School District One. **I do not want my child to have access to the Internet**. I have talked to my child and he/she understands my wishes. I understand that by denying access to my child, he/she will not be involved in instructional activities that require the use of the Internet. I request that my child be provided with alternative activities. My child understands that he/she also has a responsibility and that his/her teacher cannot be watching every minute. I hereby release the district, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my child's use of, or inability to use, the district system, including, but not limited to, claims that may arise from the unauthorized use of the system to purchase products or services. My signature below indicates that I am denying access to the following resources for my child:

_____ Internet
_____ E-mail
_____ Both Internet and E-mail

Parent's Signature: _____ **Date**: _____

Student's Signature: _____

Principal's Signature: _____ **Date**: _____

Acceptable Use Policy of Information Systems
(Policy IJNDB-R)

STATEMENT OF INTENT

Richland County School District One provides an electronic network and Internet access to enhance your educational experiences. Access to electronic and web-based resources is available through classrooms, media centers, computer labs and home computers. Through active learning experiences, students are expected to develop appropriate information literacy skills to ensure effective use of the wide variety of tools available through the network. As a network user, you are required to participate in Acceptable Use Policy training and always follow these important practices.

E-mail accounts are available to students in grades 3-12, unless denied by parents/guardians. All e-mail messages and electronic files created or stored using district resources are property of the district. Policy IJNDB and this Administrative Rule fully outline the district's intent, expectations, users' responsibilities and penalties regarding the network and its associated components.

Compliance with this policy is mandatory and includes access and use of the district information system and all peripheral devices for printing, storing, archiving and duplicating information regardless of location.

Use of the system carries a limited privacy expectation for all activities and files by all users. Parents have the right at any time to request in writing to see the contents of student e-mail and stored files.

Be aware that personal files are discoverable under the State of South Carolina's Freedom of Information Act (FOIA). Richland One has the right to place restrictions on the material accessed or posted through the system.

Access to and use of the district system is provided as a privilege, not a right. All violations of the Acceptable Use Policy and its associated Administrative Rule will be investigated and will result in one or more of the following consequences:

- Limiting, suspending or canceling use and access to the system
- Applying penalties in accordance with the Student Code of Conduct
- Levying fines and payments for damages, repairs and hardware replacement
- Application of civil or criminal liability under other applicable laws
- Expulsion

DISCLAIMER OF LIABILITY

The district makes no warranties of any kind, either expressed or implied, that the functions of the services provided by or through the district system will be error-free or without defect. The district will not be liable for the users' inappropriate use of the district's electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The district will not be responsible for ensuring the accuracy or usability of any information found on the Internet.

ACCEPTABLE USES

Student e-mail is limited to use for educational purposes. The term "educational purpose" includes classroom activities, career development, completing applications to colleges and universities, and other high-quality discovery activities as determined by the school district. Non-classroom activities, such as using e-mail to communicate with prospective colleges or universities, will at no time take precedence over classwork. For school-related business, you may download text and other non-executable files attached to e-mail messages. You are encouraged, where possible, to download large files during off-peak hours. You will check your e-mail frequently, delete unwanted messages promptly and stay within your e-mail quota. Be aware that e-mail may be deleted by system administrators at any time. You can subscribe only to high-quality discussion group mail lists at the direction of your teacher that are relevant to your education or career development. Your right to free speech, as set forth in the *"Student Code of Conduct"* applies also to using e-mail and any other form of online communication. This student e-mail system is considered a limited forum, similar to the school newspaper, and therefore the district may restrict your speech.

You will immediately notify a teacher or the system administrator if you have identified a possible security problem. Report any problems immediately.

PROHIBITED USES

Students who violate the terms of the Acceptable Use Policy or otherwise misuse the technology resources provided will be subjected to disciplinary action for a Level II offense as outlined in Section IV-I (Other Unlawful Activities) of the Richland One Student Code of Conduct. Specific prohibitions include:

- Using e-mail account for commercial purposes or political activities
- Posting chain letters or engaging in spamming
- Using e-mail for personal use, with the exception of contacting a parent/guardian for school-related or emergency purposes
- Posting personal contact information about yourself or other people (name, address, telephone, address)
- Agreeing to meet with someone you have met online without parent's/guardian's approval
- Not promptly disclosing to your teacher or other school officials any message received that is inappropriate
- Attempting to gain unauthorized access to the system or performing unauthorized functions
- Accessing another person's files
- Deliberately attempting to disrupt the information system, destroying data or spreading viruses
- Engaging in other illegal acts, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, threatening the safety of a person in an intentional or joking manner
- Sharing account information, IDs and passwords with others
- Downloading or running executable files attached to e-mail or using portable data storage devices which contain viruses or in any other way knowingly spreading computer viruses
- Using inappropriate language in public and private messages, stored files and materials on web pages
- Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or gang-related language or symbols
- Posting information that could damage or a disruption to the system
- Engaging in personal attacks or harassing another person
- Knowingly or recklessly posting false or defamatory information about another person or organization

- Accessing material that is profane, obscene, pornographic or sexually explicit, that advocates illegal acts or that advocates violence or discrimination towards other people (hate literature)
- Reposting a message that was sent to you privately without the author's permission or other activity of the information system that causes a disruption.

SOCIAL MEDIA

Richland County School District One respects the rights of its students to use social media and networking sites, message boards and forums, as well as personal websites and blogs, but it is important that a student's personal use of these sites does not damage the student's reputation or the reputation of other students or staff, pose a threat to their safety or the safety of others, and/or lead to criminal prosecution. Students should refrain from using social media to commit bullying, to post illegal activity or threatening messages, or to cheat or plagiarize. Students also should avoid posting confidential information. Parents and students should note that any such acts may lead to disciplinary action. Parents are strongly encouraged to monitor their children's Internet presence closely, and parents should understand that students are ultimately responsible for any statements disseminated from their individual social media accounts.

ATTACHMENT 3

ACCEPTABLE USE AGREEMENT FOR ALL STUDENTS

School District Five of Lexington and Richland Counties is pleased to be able to offer Internet Access for student use. Our goal in offering this access is to enhance the educational experience for our students. The Internet offers access to worldwide information in text and media form that, if properly used, will stimulate student learning. It can be a particularly powerful motivational tool for students because of the richness of the format and the depth of information resources not available through conventional means. The Student Behavior Handbook specifies guidelines for what is and is not permissible with technology. This agreement specifically addresses the privilege of using the Internet on district network systems. **The District's Student Behavior Handbook is available on the district web site, www.lexrich5.org, under the Office of Student Services. Also, Board Policy IJNDB - Use of Technology Resources can also be found online in the Board of Trustees section by clicking on Board Policies and then using the search feature for the policy manual.**

Internet Use. The Internet is an electronic highway connecting millions of computers and people around the globe. Students and teachers will have access to: electronic mail communication with people all over the world; current news; research and information databases; downloadable software and discussion groups. The District's purpose for using the Internet is to support instruction by providing access to unique resources consistent with educational objectives and the opportunity for collaborative work. School District 5 of Lexington and Richland Counties uses a technology protection measure that blocks or filters Internet access in compliance with the Children's Internet Protection Act (CIPA). This filtering device is not 100% accurate and can misclassify internet sites. Staff will monitor students' use of the Internet through software means and/or direct supervision. Students may not use the resources of School District 5 of Lexington and Richland Counties for entertainment purposes.

Students Agree To: Be polite and use appropriate language (no swearing or use of vulgarities); Practice proper system use and observe security restrictions; Understand that electronic mail (E-Mail) is NOT guaranteed to be private; Respect all electronic communications and information as private property; Use technology resources for educational purposes as appropriate to instructional assignments; Take good care of the device/computer (no food or drink near or around the device/computer).

Students Agree NOT To: Engage in any form of Cyber Bullying while using district technology resources. Cyber Bullying is defined as the use of e-mail, instant messaging, chat rooms, pagers, cell phones or other forms of information technology to deliberately harass, threaten, or intimidate someone; Use of chat rooms, instant messaging, and personal e-mail is prohibited except for designated classroom activities; Use the network in ways that would cause disruption of the use of the network by others; Use the computer to create, use or download materials which would not be permissible in District Five classrooms in any other form (i.e. obscene, profane or pornographic materials.); Use the computer, programs or files without permission; Delete programs, systems or data files without permission; Login to the computer or access

programs as any other person or allow anyone to login to your account; Share district provided user name or password with other students; Deliberately tamper with a computer system (examples: switching cables, disabling fans, introducing a virus, removing or changing keys, putting magnets on the computer, etc.); Steal or vandalize any part of the computer or network; Use the computer to tamper with, change or alter records or documents of the district; Use district computers for personal use or gain, product advertisement or political lobbying; Use public domain software and shareware beyond the provided evaluation period without properly registering and paying for same.

Enforcement of Policy

1. School District 5 of Lexington and Richland Counties uses technology protection measures that block or filter Internet access in compliance with the Children's Internet Protection Act (CIPA). This filtering device is not 100% accurate and can misclassify sites.
2. School District 5 staff will monitor students' use of the Internet through software means and/or direct supervision.

Responsibility:

District: School District Five of Lexington and Richland Counties makes no warranties of any kind for the technology resources it is providing. The District will not be responsible for any damages the student incurs including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruption. Use of any information obtained via the Internet is at the student's own risk. The District specifically denies any responsibility for the accuracy, quality, or cost of information, goods, or services obtained through the Internet.

Student: Students may utilize technology resources for educational purposes as appropriate to instructional activities. Activities that are acceptable include classroom activities, career development, and high quality research. Students may not use the resources of School District 5 of Lexington and Richland Counties for entertainment purposes. Students should practice proper system use and observe security restrictions. Security on any computer system is a high priority, especially when the system involves many users. If a student feels he/she can identify a security problem he/she should notify a school administrator.

Penalties for Improper Use:

Students who violate the terms of this Acceptable Use Agreement or otherwise misuse the technology resources provided will be subject to disciplinary action as specified in the Student Behavior Handbook. Violation of the laws of the United States or the State of South Carolina also may subject the student to criminal prosecution. If a student incurs unauthorized costs, the student will be responsible for all such costs.

Network Access

The school district provides filtered networks for employee and student use. These networks provide the most secure and safe access to the internet possible. Students may only use school

district-provided networks while on school property. Students are prohibited from bringing mobile "hot spots" on school property and prohibited from accessing any outside networks.

Parent or Guardian

As the parent or guardian of this student, I have read this Acceptable Use Agreement. I understand that this access to technology is designed for educational purposes and that School District Five of Lexington and Richland Counties has taken precautions to limit access to controversial material. However, I recognize it is impossible for the district to restrict access to all materials which I might deem controversial, and I will not hold the district responsible for materials acquired on the network. Further, I accept responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission for my child to use a school account for independent navigation and certify that the information contained on this form is correct. I understand that teachers or media specialists who are exploring World Wide Web sites with a class do not need special permission for such activity if the faculty member is in control of the navigation to known educational sites. A student who is using the internet at the constant direction of the faculty member is not "independently" navigating the internet. This circumstance does not require special parental permission.

I understand the guidelines and disciplinary actions listed in the District's Student Behavior Handbook for what is and is not permissible with technology, as well as Board Policy IJNDB, which details the Use of Technology Resources.

ATTACHMENT 4

Richland School District
Acceptable Use Policy

Internet access is available to all students who agree to follow these guidelines. Parents/Guardians have the right to decline District Internet access for their student and are required to communicate their wishes by completing the opt-out form below.

We are pleased to offer students of the Richland School District use of the District computer network, including Internet access. The Internet will enable students to explore thousands of libraries, databases, and educational resources throughout the world. Families should be warned that material found on the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make the Internet available to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from the Internet in the form of information resources and opportunities for collaboration exceed any disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media information sources. To that end, the Richland School District supports and respects each family's right to decide whether or not to allow Internet access.

DISTRICT INTERNET GUIDELINES:

1. Students are responsible for good behavior and communications on school computer networks. Communications on the network are public in nature. Therefore, general school and District rules for behavior and communications apply.
2. The network is provided to students for research purposes as long as the student agrees to act in a responsible manner.
3. Access to the computers is a privilege, not a right, and entails responsibility.
4. It is presumed that students will comply with District standards and Network Code of Conduct, and understand that disciplinary procedures will result if they fail to do so.
5. While complying with the Children's Internet Protection Act (CIPA – internet filtering) and making every attempt to supervise students while accessing Internet resources, the District is not responsible for restricting, monitoring, or controlling the communications of individuals utilizing the network.
6. Network storage areas may be treated like school lockers. Therefore, network administrators may review user files and communications to maintain system integrity and insure that users are using the system responsibly. Users should have no expectations of privacy in their electronic files stored on Richland School District computers.
7. All use of the system must be in support of education and research and consistent with the mission of the District.

Students using the District network are not permitted to do the following:

- Access, send, or display offensive messages or pictures
- Use obscene or defamatory language
- Harass, insult, defame or attack others
- Damage computers, alter computer systems or computer networks
- Download/install programs, files, etc. without permission
- Access chat rooms, instant messaging services, games, etc.
- Violate copyright laws
- Use another's network account/password
- Give out his/her name, address, or phone number
- Trespass in another's folder, work or files
- Intentionally waste limited resources
- Employ the network for commercial purposes
- Accessing personal e-mail accounts is only allowed for uses outlined in the classroom curriculum

DISCIPLINE

Violations may result in loss of access to the Internet, loss of computer usage while at school, as well as other disciplinary or legal action.

Please fill out and return the bottom form to the school. You may keep the top portion for your own records.

Richland School District Opt-Out Form

Parent notification to _____*(current school)* declining Internet access privileges for the following child:

Student Name: _____ **Grade Level:** _____

As the parent/guardian of the student above, I **decline permission** for my child to access the Internet at school. I am aware that this request needs to be updated on a yearly basis. If at any time I would like my child to be able to access the Internet while at school, I am aware that such permission will need to be made in writing and submitted to the school office.

Parent/Guardian Signature: _____ **Date:** _____

Address: _____ **Home Phone Number:** _____

Note: Please be aware that some library databases, periodicals, etc., classroom resource materials, and supplemental instructional materials, at all schools are accessed via the Internet. By signing this form you are denying your student access to these District resources.

ATTACHMENT 5

Consumer Guide

Children's Internet Protection Act (CIPA)

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011.

What CIPA requires

Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them.

Schools and libraries must certify they are in compliance with CIPA before they can receive E-rate funding.

- CIPA does not apply to schools and libraries receiving discounts only for telecommunications service only;
- An authorized person may disable the blocking or filtering measure during use by an adult to enable access for bona fide research or other lawful purposes.
- CIPA does not require the tracking of Internet use by minors or adults.

You can find out more about CIPA or apply for E-rate funding by contacting the Universal Service Administrative Company's (USAC) Schools and Libraries Division (SLD) at www.sl.universalservice.org. SLD also operates a client service bureau to answer questions at 1-888-203-8100 or via email through the SLD website.

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · www.fcc.gov/consumer-governmental-affairs-bureau

Filing a complaint

You have multiple options for filing a complaint with the FCC:

- File a complaint online at https://consumercomplaints.fcc.gov
- By phone: 1-888-CALL-FCC (1-888-225-5322); TTY: 1-888-TELL-FCC (1-888-835-5322); ASL: 1-844-432-2275
- By mail (please include your name, address, contact information and as much detail about your complaint as possible):

  Federal Communications Commission
  Consumer and Governmental Affairs Bureau
  Consumer Inquiries and Complaints Division
  445 12th Street, S.W.
  Washington, DC 20554

Accessible formats

To request this article in an accessible format - braille, large print, Word or text document or audio - write or call us at the address or phone number at the bottom of the page, or send an email to fcc504@fcc.gov.

Last Reviewed: 11/03/15

ATTACHMENT 6

NIST Special Publication 800-167

Guide to Application Whitelisting

Adam Sedgewick
Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-167

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-167

Guide to Application Whitelisting

Adam Sedgewick
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-167

October 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.*, Public Law 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-167
Natl. Inst. Stand. Technol. Spec. Publ. 800-167, 24 pages (October 2015)
CODEN: NSPUE2

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-167

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

An application whitelist is a list of applications and application components that are authorized for use in an organization. Application whitelisting technologies use whitelists to control which applications are permitted to execute on a host. This helps to stop the execution of malware, unlicensed software, and other unauthorized software. This publication is intended to assist organizations in understanding the basics of application whitelisting. It also explains planning and implementation for whitelisting technologies throughout the security deployment lifecycle.

Keywords

access control; application control; application whitelisting; information security; software security; whitelisting

Acknowledgments

The authors, Adam Sedgewick and Murugiah Souppaya of the National Institute of Standards and Technology (NIST) and Karen Scarfone of Scarfone Cybersecurity, wish to thank their colleagues, in particular Eric Chudow from the National Security Agency, who contributed to this publication, as well as the reviewers who provided feedback.

Table of Contents

List of Appendices

Executive Summary

An *application whitelist* is a list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline. The technologies used to apply application whitelists—to control which applications are permitted to install or execute on a host—are called *whitelisting programs*, *application control programs,* or *application whitelisting technologies*. Application whitelisting technologies are intended to stop the execution of malware and other unauthorized software. Unlike security technologies such as antivirus software, which block known bad activity and permit all other, application whitelisting technologies are designed to permit known good activity and block all other. The purpose of this publication is to assist organizations in understanding the basics of application whitelisting and planning for its implementation.

Implementing the following recommendations should facilitate more efficient and effective application whitelisting use for federal departments and agencies.

Consider using application whitelisting technologies already built into the host operating system.

Organizations should consider these technologies, particularly for centrally managed desktops, laptops, and servers, because of the relative ease in managing these solutions and the minimal additional cost. If built-in application whitelisting capabilities are not available or are determined to be unsuitable, then the alternative is to examine third-party solutions with robust centralized management capabilities.

Use products that support more sophisticated application whitelisting attributes.

Choosing attributes is largely a matter of achieving the right balance of security, maintainability, and usability. Simpler attributes such as file path, filename, and file size should not be used by themselves unless there are strict access controls in place to tightly restrict file activity, and even then there are often significant benefits to pairing them with other attributes. A combination of digital signature/publisher and cryptographic hash techniques generally provides the most accurate and comprehensive application whitelisting capability, but usability and maintainability requirements can put significant burdens on the organization.

Test prospective application whitelisting technology in monitoring mode.

It is highly recommended to test any prospective application whitelisting technology in a monitoring mode to see how it behaves before solution deployment. This testing should include a thorough evaluation of how the solution reacts to changes in software, such as installing an update. An application whitelisting technology might be considered unsuitable if, for instance, it had to be disabled in order to install security updates for the operating system or particular applications.

Address application whitelisting technology planning and deployment in a phased approach.

A successful deployment will require a clear, step-by-step planning and implementation process. The use of a phased approach for deployment can minimize unforeseen issues and identify potential pitfalls early in the process. This model also allows for incorporating advances in new technology and adapting the technology to the ever-changing enterprise. In addition to following the security recommendations presented in this publication, organizations implementing application whitelisting technologies should also follow the recommendations from NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, which defines minimum recommended management, operational, and technical controls for information systems based on impact categories.

When evaluating the possibility of deploying application whitelisting, analyze the environment or environments in which the application whitelisting will be running.

It is more practical to implement whitelisting on hosts that are centrally managed and have a consistent application workload. Application whitelisting solutions are generally strongly recommended for hosts in high-risk environments where security outweighs unrestricted functionality. Suitability for typical managed environments depends on how tightly the hosts are managed and the extent of the risks that they face. Organizations considering application whitelisting deployment in a typical managed environment should perform a risk assessment to determine whether the security benefits provided by application whitelisting outweigh its possible negative impact on operations. Organizations should also be mindful that they will need dedicated staff managing and maintaining the application whitelisting solution depending on the scale and specifics of the solution implemented, similar to handling an enterprise antivirus or intrusion detection solution. An organization that can dedicate the necessary trained staff to solution maintenance and has built-in application whitelisting technology should generally implement application whitelisting at least in a monitoring mode.

1. Introduction

1.1 Purpose and Scope

The purpose of this publication is to assist organizations in understanding the basics of application whitelisting (also known as application control). All other forms of whitelisting, such as email, network traffic, and mobile code whitelisting, are out of the scope of this publication.

1.2 Audience

This document is intended for security managers, engineers, administrators, and others who are responsible for acquiring, testing, implementing, and maintaining application whitelisting technologies.

1.3 Document Structure

The remainder of this document is organized into the following sections and appendices:

- Section 2 examines the basics of application whitelisting.
- Section 3 explains planning and implementation for application whitelisting technologies throughout the security deployment lifecycle.
- Appendix A provides a mapping to existing standards and guidelines that support using application whitelisting technologies.
- Appendix B discusses considerations involved in applying application whitelisting technologies to mobile platforms.
- Appendix C defines selected acronyms and abbreviations used in the document.
- Appendix D provides a bibliography for the publication.

2. The Basics of Application Whitelisting

A *whitelist* is a list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline. A *blacklist* is a list of discrete entities that have been previously determined to be associated with malicious activity. A *graylist* is a list of discrete entities that have not yet been established as benign or malicious; more information is needed to move graylist items onto a whitelist or a blacklist. Whitelists, blacklists, and graylists are primarily used as a form of access control: permitting activity corresponding to the whitelist and not permitting activity corresponding to the blacklist. Graylist treatment depends on the type of entities it contains. An example of how a graylist might be handled is prompting the user to make a decision or notifying an administrator that the entity needs to have its security evaluated before use.

An *application whitelist* is a list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline. The technologies used to enforce application whitelists—to control which applications are permitted to be installed or executed on a host—are called *whitelisting programs*, *application control programs,* or *application whitelisting technologies*. Application whitelisting technologies are intended to stop the execution of malware and other unauthorized software. Unlike security technologies such as antivirus software, which use blacklists to block known bad activity and permit all other, application whitelisting technologies are designed to permit known good activity and block all other.

This section examines the basics of application whitelisting. It first discusses the categories of threats that application whitelisting can mitigate and the types of application whitelisting. Next, it defines the types of operational runtime modes available for application whitelisting technologies. The section also explains the motivations for application whitelisting and discusses uses of application whitelisting technologies other than application access control. Finally, the section concludes by examining differences in deployment based on operational environment, as well as considerations for evaluating the relative effectiveness of application whitelisting solutions.

2.1 Threats

As previously discussed, application whitelisting software prevents installation and/or execution of any application that is not specifically authorized for use on a particular host. This mitigates multiple categories of threats, including malware and other unauthorized software.

Malware, also known as malicious code, refers to an application that is covertly inserted into another piece of software (e.g., operating system, application) with the intent to steal or destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.[1] Many of today's threats are malware-based, attempting to infect hosts (install their malicious code) and execute on those hosts to steal their data or perform other harmful activities. When properly configured, application whitelisting technologies can stop most malware from being executed (and often from being installed in the first place). Application whitelisting technologies can be significantly more effective at stopping unknown malware threats than conventional antivirus software and other traditional antimalware security controls. This is important because today's malware threats are increasingly customized and targeted, making traditional detection technologies largely ineffective.

[1] This definition is based on the one provided in NIST Special Publication (SP) 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* (July 2013). http://dx.doi.org/10.6028/NIST.SP.800-83r1.

The other major category of threats that application whitelisting technology can mitigate is other unauthorized software (unauthorized software besides malware). This software can pose multiple problems. For example, it can introduce unmanaged vulnerable software into the environment, which can then be used by attackers to exploit hosts and further compromise them. There can also be legal issues with the installation of unauthorized software, such as violations of licensing agreements.

Application whitelisting is most readily used to stop threats on managed hosts where users are not able to install or run applications without authorization. An example is a kiosk workstation where users are limited to running a web browser; installation and execution of all applications other than the selected web browser and authorized application-based security controls (such as antivirus software) would be prohibited. Another example is a laptop that has all authorized applications preinstalled for the user, and the user does not have the administrative privileges necessary to install additional applications or disable the application whitelisting software. Application whitelisting may also be beneficial on servers, particularly if there is concern about malware spreading to these servers from other hosts (e.g., administrator laptops).

2.2 Types of Application Whitelisting

This section discusses the types of application whitelisting. This includes the application file and folder attributes that can be analyzed; the types of application resources handled, such as executables, libraries, and scripts; and techniques for whitelist generation.

2.2.1 File and Folder Attributes

Application whitelisting can be based on a variety of application file and folder attributes, including the following:[2]

- **File path.** This is the most general attribute: to permit all applications contained within a particular path (directory/folder). Used by itself, this is a very weak attribute, because it allows any malicious files placed within the directory to be executed. However, if the path is protected by strict access controls that only allow authorized administrators to add or modify files, this becomes a stronger attribute. Paths can be beneficial by not requiring each file within the path to be listed separately, which reduces the need to update the whitelist for every new application and patch.
- **Filename.** This attribute, for the name of an application file, is too general to be used on its own. If a file were to become infected or be replaced, its name would be unchanged so the file would still be executed under the whitelist. Also, an attacker could simply place a malicious file onto a host and use the same name as a common benign file. Because of these weaknesses, this attribute should not be used on its own; rather, it should be paired with other attributes. For example, it would be stronger to combine path and filename attributes with strict access controls or to combine a filename attribute with a digital signature attribute (described below).
- **File size.** This attribute is typically used only in combination with other attributes, such as filename. Monitoring the file size assumes that a malicious version of an application would have a different file size than the original; however, attackers can craft malicious files to have the same length as their benign counterparts. Other attributes, such as digital signature and cryptographic hash, provide

[2] This list of attributes is not intended to be all-inclusive. Also, it is expected that new forms of attributes may arise as technologies advance. Another set of attributes is the *software identification tags (SWID tags)* which define unique information about an installed software application, including its name, edition, version, whether it's part of a bundle and more (http://tagvault.org/swid-tags/).

substantially better unique identification of files than file size does, and should be used instead of file size whenever feasible.

- **Digital signature or publisher.** Application files are increasingly being digitally signed by their publishers. A digital signature provides a reliable, unique value for an application file that is to be verified by the recipient to ensure that the file is legitimate and has not been altered. Unfortunately, many application files are not yet signed by their publishers, so using only publisher-provided digital signatures as attributes is generally not feasible. Some application whitelists can be based on verifying the publisher's identity instead of verifying individual digital signatures; this is based on the assumption that all applications from trusted publishers can themselves be trusted.[3] This assumption may be faulty if the software vendor has multiple applications and the organization wants to restrict which of those applications can be executed. Also, relying on the publisher's verified identity only would allow older software versions with known vulnerabilities to be executed. However, the benefit of basing a whitelist on publisher identities is that the whitelist only needs updates when there is a new publisher (i.e., software vendor) or when a publisher updates its signature key.[4]
- **Cryptographic hash.** A cryptographic hash provides a reliable, unique value for an application file, so long as the cryptography being used is strong and the hash is already known to be associated with a good file. Cryptographic hashes are accurate no matter where the file is placed, what it is named, or how it is signed. However, a cryptographic hash is not helpful when a file is updated, such as when an application is patched; the patched version will have a different hash. In these cases the patch should be identified as legitimate through its digital signature, then its cryptographic hash should be added to the whitelist. Note that if the whitelist is not continuously updated with new hashes for new and updated applications, there is a significant risk of software not functioning correctly, and if the whitelist is not continuously updated to remove existing hashes for older software versions with known vulnerabilities, there is a significant risk of vulnerable software being allowed to run.

As the discussions above indicate, choosing attributes is largely a matter of achieving the right balance of security, maintainability, and usability. Simpler attributes such as file path, filename, and file size should not be used by themselves unless there are strict access controls in place to tightly restrict file activity, and even then there are often significant benefits to pairing them with other attributes. A combination of digital signature/publisher and cryptographic hash techniques generally provides the most accurate and comprehensive application whitelisting capability, but usability and maintainability requirements can put significant burdens on the organization.

2.2.2 Application Resources

Application whitelisting is most often associated with monitoring executables. However, most application whitelisting technologies also have the ability to monitor at least some other types of application-related files, such as libraries, scripts, macros, browser plug-ins (or add-ons or extensions), configuration files, and application-related registry entries (on Windows hosts). The granularity of this monitoring varies significantly among application whitelisting technologies; for example, some can only permit or block whole classes of scripts (e.g., JavaScript)[5], while others can permit or block individual scripts within a class of scripts.

---

[3] For its internal applications, an organization can issue its own internal signing key to anchor its root of trust, instead of depending on a signing key from an external publisher.

[4] An alternative approach is to employ cross-signing, where both the software vendor and the organization sign each application, thus indicating that it is both authentic and approved by the organization.

[5] Generally this means that the application is blocking the executable for the scripting language, instead of blocking the scripts themselves.

2.2.3 Whitelist Generation and Maintenance

There are two primary methods of generating an application whitelist for a host. One is to use vendor-provided information on the characteristics of known good applications, supplemented with organization-generated information on the characteristics of organization-specific applications (i.e., in-house custom applications). The other method of generating an application whitelist is to scan the files on a clean host[6] to build a good known baseline.[7]

Both of these methods are effective on their own, except when applications are updated (e.g., patched) or new applications are installed. If the vendor is providing the whitelist information, the vendor will have to acquire the patch or new application, record its files' characteristics, and send the corresponding information to customers. If the organization is building its own whitelist information, it will have to: acquire each patch or new application, record its files' characteristics, and update its whitelists with the new information; or, redo its known good baseline to serve as the new reference baseline. Any of these methods may cause problematic delays for organizations that apply patches quickly, especially automatically; patched software may be seen as unknown software and prohibited from running. Certain attributes, such as file path and publisher, generally do not change with each patch and so whitelists utilizing those attributes do not need to be updated as often and should cause fewer of these delays.

To avoid these problems with updates, most application whitelisting technologies offer maintenance options. For example, many technologies allow the administrator to select certain services (e.g., patch management software) to be trusted updaters. This means that any files that they add to or modify on a host are automatically added to the whitelist. Similar options are available for designating trusted publishers (i.e., software vendors), users (e.g., system administrators), sources (e.g., trusted network paths), and other trusted entities that may update whitelists.

Another option available with some application whitelisting technologies is the use of reputation services. These services determine if a service, publisher, or other external entity is generally associated with benign or malicious content. This allows application whitelisting software to make decisions about how to handle new or modified files based on the reputation of the associated service, publisher, etc., instead of simply adding them to a graylist for subsequent manual processing.

2.3 Application Whitelisting Modes

Most application whitelisting technologies offer two operational runtime modes:

- **Audit mode** allows items, including those not on the whitelist to be executed and logs their execution. This mode provides data for continuous monitoring processes to analyze.
- **Enforcement mode** automatically permits execution of whitelisted items and/or blocks execution of blacklisted items. There are different forms of enforcement mode, which are differentiated by how they handle items that are not whitelisted or blacklisted. These forms include the following:
    - **Whitelist enforcement** permits only whitelist items to be executed and blocks execution of all others;

[6] "Clean host" refers to a host with an operating system installation that has never been accessed by end users, such as a host freshly built from a fully-patched security baseline image. Using anything other than a clean host for whitelist generation poses significant risks of inadvertently categorizing malware on the host as whitelisted software.

[7] NIST hosts the National Software Reference Library (NSRL), which contains metadata for application files for forensic investigation purposes. See http://www.nsrl.nist.gov/ for additional information.

- **User prompting** asks the user (or, in some cases, the administrator) to accept or reject each attempt to execute a file that is not whitelisted or blacklisted; and
- **Blacklist enforcement** blocks execution of blacklisted items but allows everything else to be executed.

An application whitelisting technology run in audit mode is strictly informative; it can log the execution of malware and other unauthorized executables, but it cannot do anything to stop them. Audit mode is primarily intended for use when first deploying an application whitelisting technology, to help an organization evaluate and fine-tune the technology before switching it to enforcement mode.

Many application whitelisting technologies have granular options for setting modes. Some features could be configured to run in enforcement mode while other features run in audit mode. For example, Windows registry changes might be permitted (audit mode) while operating system file changes would be prohibited (enforcement mode). Some products also support multiple enforcement modes and allow granular setting of those for different types of monitored entities.

2.4 Uses of Application Whitelisting Technologies

As stated in the Section 2 introduction, the primary purpose of application whitelisting technologies is to provide application access control, i.e., to stop the execution of unauthorized software. However, most application whitelisting technologies can be used for other purposes as well, including the following:

- **Software inventory.** Application whitelisting technologies can keep an inventory of the applications and application versions installed on each host. This allows an organization to identify unauthorized applications—unlicensed applications, prohibited applications, etc.—as well as to identify "wrong" versions of software (both too old and too new). This software inventory capability is also useful for forensic investigations, such as finding modified applications, unauthorized applications, malware, unknown applications, etc. on a given host.
- **File integrity monitoring.** Most application whitelisting technologies can perform frequent or continuous monitoring of attempted changes to application files. Some technologies can prevent files from being changed, while other technologies cannot prevent changes but can immediately report when changes occur.
- **Incident response.** An organization responding to an incident on a host could capture the characteristics of the malicious files on that host (e.g., generate cryptographic file hashes) and use application whitelisting technologies to check other hosts for the same files, indicating that they have been compromised as well.

Some application whitelisting technologies may have additional capabilities, including the following:

- Access control for portable storage devices, such as restricting file reads, writes, and executes for all files on removable media; only permitting the use of encrypted devices; and only permitting the use of drives with particular serial numbers.
- Memory protection, primarily involving stopping certain attacks (e.g., buffer overflows) that directly affect files in memory, not files in storage. Most application whitelisting technologies only focus on the files in storage, but do not ensure that the files in memory are not altered or exploited.
- Software reputation services, such as reviewing what other software a particular application is often bundled with, and determining if an application is known to pose a substantial security risk.

- Anti-malware technology integration; for example, attempting to identify known malicious content by running graylisted files through an online scanner with many antivirus scanning engines or other types of malware analysis products. Malware analysis products can inform application whitelisting decision making processes.

2.5 Operational Environment Differences

As discussed in NIST SP 800-70 Revision 2, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*,[8] there are significant differences among operational environments. These differences are important in terms of selecting and deploying application whitelisting technologies. The major categories of operational environments are as follows:

- **Standalone.** Also referred to as **Small Office/Home Office (SOHO)**, a Standalone environment refers to a small, informal computer installation that is used for home or business purposes. For technical and business (economic) reasons, Standalone environment hosts are generally not managed remotely. Standalone environments are typically the least secured.
- **Managed**. The Managed environment, also called an **Enterprise** environment, typically contains large organizational systems with defined suites of hardware and software configurations, usually consisting of centrally managed IT products (e.g., workstations and servers). The managed nature of these environments gives administrators centralized control over various settings on IT products. Because of the supported and largely homogeneous nature of the Managed environment, it is typically easier to use more functionally restrictive settings in Managed environments than in Standalone environments.
- **Specialized Security-Limited Functionality (Custom)**. A Custom environment contains systems in which the functionality and degree of security do not fit the Standalone or Managed environments. Specialized Security-Limited Functionality (SSLF) is a Custom environment that is highly restrictive and secure; it is usually reserved for hosts that have the highest threats and associated impacts. Because hosts in an SSLF environment are at high risk of attack or data exposure, security takes high precedence over functionality.

2.6 Evaluating Application Whitelisting Solutions

The first step in evaluating the possibility of deploying an application whitelisting solution should be an analysis of the environment or environments in which the hosts will be running. Generally it is not feasible to implement whitelisting on Standalone environment hosts because of the lack of centralized management. Application whitelisting solutions are generally strongly recommended for hosts in SSLF environments because of the high risks that they face. Suitability for Managed environments depends on how tightly the hosts are managed and the extent of the risks that they face; organizations considering application whitelisting deployment in a Managed environment should perform a risk assessment to determine whether the security benefits provided by application whitelisting outweigh its possible negative impact on operations. Organizations should also be mindful that they will need dedicated staff managing and maintaining the application whitelisting solution, similar to handling an enterprise antivirus or intrusion detection solution.

Once it has been determined that application whitelisting technologies are merited for a particular environment, the next step is to consider which technologies might be feasible. Organizations should consider application whitelisting technologies already built into the operating system, particularly for centrally managed hosts (e.g., desktops, laptops, servers), because of the relative ease and minimal

[8] http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf

additional cost in managing these solutions. If built-in application whitelisting capabilities are not available or are determined to be unsuitable, then the alternative is to examine third-party solutions with robust centralized management capabilities. An organization that can dedicate the necessary trained staff to solution maintenance and has built-in application whitelisting technology should generally implement application whitelisting at least in a monitoring mode.

It is highly recommended to test any prospective application whitelisting technology in a monitoring mode to see how it behaves before solution deployment. This testing should include a thorough evaluation of how the solution reacts to changes in software, such as installing an update. An application whitelisting technology might be considered unsuitable if, for instance, it had to be disabled in order to install security updates for the operating system or particular applications.

2.7 Additional Considerations

This section describes additional considerations that organizations should examine when evaluating the likely effectiveness of potential application whitelisting technology solutions.

Effectiveness Consideration	Further Explanation
How easily can a solution be bypassed?	If a solution can be bypassed easily, some users will choose to do so in order to run unauthorized software, and malware may take advantage of the configuration weakness to execute on the host.
How complex is a solution (hash-based versus signature-based, etc.)?	Generally, more complex solutions will be harder for an attacker to circumvent. A relatively simple solution lacks the features necessary to minimize false positives and false negatives. However, more complex solutions may have higher administrative and maintenance overhead.
What are the relative costs of a solution?	It is important to consider not only the implementation costs of a solution, but also the ongoing operational costs. The implementation and operational costs of solutions may vary widely.
What impact does the solution have on standard performance?	Using application whitelisting technologies generally should not be noticeable to users in terms of significantly slowing host performance.
What impact does the solution have on business/mission?	If the solution does not minimize false positives, users may frequently be prevented from running authorized software. If the solution does not minimize false negatives, malware infections are more likely to occur. Both of these circumstances could seriously impact the organization's mission, depending on the value of the relevant hosts.
How usable is the solution for both users and administrators?	A more usable solution will not only minimize false positives, to minimize user disruption, but it will also provide pertinent information to users and administrators when software is blocked from installation or execution.
What are the long-term maintenance demands for running the solution?	As new applications are added to the environment and existing applications are updated, there may be technical difficulties in keeping whitelists updated in a timely manner, and significant costs associated with maintenance. Certain types of whitelisting require more frequent whitelist changes than others. However, the amount of maintenance needed must be balanced with the effectiveness of the solution; a higher-maintenance solution that prevents more incidents may actually be less expensive in the long term since it includes the cost to remediate incidents, versus a lower-maintenance solution that has limited effectiveness in stopping threats.

3. Application Whitelisting Planning and Implementation

This section discusses considerations for planning and implementing application whitelisting technologies for end user devices. As with any new technology deployment, application whitelisting technology planning and implementation should be addressed in a phased approach. A successful deployment can be achieved by following a clear, step-by-step planning and implementation process. The use of a phased approach for deployment can minimize unforeseen issues and identify potential pitfalls early in the process. This model also allows for incorporating advances in new technology and adapting the technology to the ever-changing enterprise. The following is an example of planning and implementation phases:

1. **Initiate the Solution.** The first phase involves identifying current and future needs for application whitelisting; specifying requirements for performance, functionality, and security; and developing necessary policies.

2. **Design the Solution.** The second phase involves all facets of designing the application whitelisting solution. Examples include architectural considerations, whitelist management, cryptography policy, and security aspects of the solution itself.

3. **Implement and Test a Prototype.** The next phase involves implementing and testing a prototype of the designed solution in a lab or test environment. The primary goals of the testing are to evaluate the functionality, management, performance, and security of the solution.

4. **Deploy the Solution.** Once the testing is completed and all issues are resolved, the next phase includes the gradual deployment of the application whitelisting technology throughout the enterprise.

5. **Manage the Solution.** After the solution has been deployed, it is managed throughout its lifecycle. Management includes solution maintenance and support for operational issues. The lifecycle process is repeated when enhancements or significant changes need to be incorporated into the solution.

This document does not describe the planning and implementation process in depth because the same basic steps are performed for any security technology. This section only highlights those considerations that are of particular interest for application whitelisting technologies.[9] These considerations are not intended to be comprehensive, nor is there any implication that particular security elements not listed here are unimportant or unnecessary. In addition to following the security recommendations presented in this publication, organizations implementing application whitelisting technologies should also follow the recommendations from NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*[10], which defines minimum recommended management, operational, and technical controls for information systems based on impact categories.

3.1 Initiation

The purpose of this phase is to identify the current and future needs for application whitelisting and to determine how those needs can best be met. Requirements specific to application whitelisting that should

[9] Section 3 only addresses application whitelisting technology planning and implementation, not other phases such as solution retirement, because there is nothing unique to application whitelisting to discuss for other phases. Organizations can simply follow their existing processes for solution retirement and for any other security technology phases.

[10] http://dx.doi.org/10.6028/NIST.SP.800-53r4

be considered include the following:

- **External Requirements.** The organization may be subject to oversight or review by another organization that requires application whitelisting.
- **System and Network Environments.** It is important to understand the characteristics of the organization's system and network environments to select compatible application whitelisting solutions with the necessary functionality. Aspects to consider include the following:
  - Characteristics of the devices that need application whitelisting, especially the operating systems (OSs) and applications; and
  - Technical attributes of the interfaces of other systems with which the application whitelisting solution might be integrated, such as centralized logging servers and security information and event management (SIEM) software.

The outcome of the organization's requirements analysis should be a determination of the types of applications or application components (executables, libraries, registry entries, configuration files, etc.) that need to be monitored; the types of threats the application whitelisting should protect against (Section 2.1); and the types of application whitelisting that should be used to balance security, usability, and maintainability (Section 2.2). For example, the organization may decide to block execution of all unauthorized application components on higher-risk client systems, while monitoring (but not blocking) execution of unauthorized application components on lower-risk client systems. These decisions should be captured in policy.

Another outcome of the analysis is the documentation of the requirements for the application whitelisting technologies themselves, including security capabilities (e.g., authentication, cryptography, key management), performance requirements, management requirements (including reliability, interoperability, and scalability), the security of the technology itself, usability, and maintenance requirements (e.g., applying updates).

In many cases, a single application whitelisting product cannot meet all of the organization's identified needs. For example, the organization may need to monitor applications on devices running several different OSs, yet no appropriate product can work on all those platforms. Also, some operating systems may have application whitelisting technologies built-in. Organizations can solve this problem in several ways, such as acquiring multiple products or replacing older devices. Organizations should ensure that effective solutions are identified for all the types of end user devices that need their applications monitored, if possible, and that a waiver and risk management process is created for unusual cases that cannot be addressed by the identified solutions.

Examples of challenging platforms for application whitelisting include mobile devices[11] and industrial control systems (ICS)[12]. One of the main benefits of using mobile devices is being able to acquire a wide variety of applications easily, quickly, and cheaply (often free). Unfortunately, this philosophy makes it infeasible in many cases to implement whitelisting for mobile devices. If mobile devices are tightly managed, much like some desktops or laptops, and only allowed to acquire approved apps from an enterprise-sponsored app store, then whitelisting may be practical, but for user-controlled unmanaged mobile devices, whitelisting may not be an option as of this writing.

---

[11] For more information on mobile device security, see NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (http://dx.doi.org/10.6028/NIST.SP.800-124r1).

[12] More information on ICS is available from NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security* (http://dx.doi.org/10.6028/NIST.SP.800-82r2).

An ICS is a challenging platform for whitelisting in part because, unlike most other computing devices, ICSs strongly favor availability over confidentiality. It is critical that ICSs continue to function properly no matter what is happening to them, including cyber attacks. Because application whitelisting can inadvertently prevent benign applications from being executed, its use for ICSs must be carefully analyzed and tested for feasibility. Another problem with ICSs is that they often use atypical platforms, which may not be supported by any acceptable application whitelisting solutions. However, since ICSs are used for specific functionality and run only certain ICS software, in some cases they are actually easier to whitelist than more dynamic, heterogeneous environments.

3.2 Design

Once the needs have been identified and the appropriate application whitelisting technologies have been chosen, the next phase is to design a solution that meets those needs. If these design decisions are incorrect, then the application whitelisting implementation will be more susceptible to compromise and failure. Major aspects of solution design that are particularly important for application whitelisting are as follows:

- **Cryptography.** Cryptography is used in at least three ways for application whitelisting technologies: 1) to generate and verify cryptographic hashes for files and other application components; 2) to validate digital signatures for files; and 3) to protect the confidentiality and integrity of communications between individual hosts and centralized management (for example, encrypting lists of installed applications and application versions). For all of these functions, Federal agencies must use Federal Information Processing Standard (FIPS) approved or NIST-recommended algorithms contained in validated cryptographic modules.[13] Organizations should consider how easily the solution can be updated when stronger algorithms and key sizes become available in the future.
- **Solution architecture.** The architecture of the application whitelisting technology refers to the selection of devices and software to provide application whitelisting services and the placement of centralized elements within the existing network infrastructure, such as management servers. Most application whitelisting technologies can only operate as a centrally managed solution; there may be copies of whitelists on individual hosts, but enterprise management is centralized. Each end user device must have software that provides application whitelisting enforcement or auditing. Designing the architecture includes component placement, redundancy, reliability, and interoperability.
- **Whitelist management.** As discussed in Section 2.2.3, whitelist management can involve the establishment of trusted publishers, users, updaters, etc. Organizations should choose these trusted entities carefully because a compromise in a trusted entity could lead to the compromise of the application whitelisting technology, and consequently to the hosts it protects. However, failure to identify necessary entities as trusted will likely lead to operational problems, such as when files updated by patch installation are not automatically trusted by the application whitelisting technology.

3.3 Prototype Testing

After the solution has been designed, the next step is to implement and test a prototype of the design. Ideally, implementation and testing should first be performed on lab or test devices. Only solutions in the final phase of testing should be implemented on production devices. Aspects of the prototype solution that require evaluation include the following:

[13] For more information on validated implementations of cryptographic algorithms and modules, see http://csrc.nist.gov/groups/STM/cavp/ and http://csrc.nist.gov/groups/STM/cmvp/, respectively.

- **Application control functionality.** Basic functionality will need to be checked during the prototype testing. Examples include allowing the execution of whitelisted applications, blocking the execution of blacklisted applications, and detecting modifications to whitelisted applications. These functions should be verified by: installing patches and other updates; manually modifying executables; and making other changes to applications to confirm that the application control policies can be properly enforced and cannot be easily circumvented.
- **Management.** Administrators should be able to configure and manage all components of the solution effectively and securely. It is particularly important to evaluate the ease of deployment and configuration, including how easily the solution can be managed as the solution is scaled to larger deployments. Management concerns should include the effects of patching/upgrading the application whitelisting software, changing software settings (e.g., changing cryptographic algorithms or key sizes), and managing cryptographic keys. Another important management concern that needs special attention is whitelist generation and maintenance, such as how the whitelists accommodate software patching.
- **Logging/alerting.** The logging, alerting, and data management functions should work properly in accordance with the organization's policies and strategies.
- **Performance.** The solution should be able to provide adequate performance during normal and peak usage. Testing should incorporate a variety of devices, OSs, and applications.
- **Security of the implementation.** The application whitelisting technology itself may contain vulnerabilities and weaknesses that attackers could exploit. Organizations with high security needs may want to perform extensive vulnerability assessments against the application whitelisting components.[14]

Before installing application whitelisting software on a host, organizations should scan the host for malware and either remove any malware that is detected or rebuild the host. The scan will ensure that malware files are not included in the whitelist generation process. Organizations should also ensure that the host's OS is secured properly, including that it is fully patched and that other necessary security controls are installed and configured properly. If the OS is not secured properly, the host is more likely to be compromised, which could weaken the protection provided by the application whitelisting technology.

3.4 Deployment

Once testing is complete and any issues have been resolved, the next phase of the planning and implementation model involves deploying the solution. When the components are being deployed into production, organizations should initially use application whitelisting on a small number of hosts. Deploying it to many hosts at once might overwhelm the management servers or identify other bottlenecks through loss of availability. Many of the problems that occur are likely to occur on multiple hosts, so it is helpful to identify such problems either during the testing process or when deploying the first hosts, so that those problems can be addressed before widespread deployment. A phased deployment provides administrators an opportunity to evaluate the impact of the solution and resolve issues prior to enterprise-wide deployment. It also provides time for the IT staff (e.g., system administrators, help desk) and users to be trained and to become accustomed to the operational lifecycle of the implementation.

Most of the issues that can occur during deployment are the same types of issues that occur during any large IT deployment. In addition to potential problems described earlier in this publication, another

[14] For more information on the fundamentals of testing and assessing security, see NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* (http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf).

typical issue is end users discovering and disabling the application whitelisting software. Many products run in a stealth mode so that users cannot readily tell that they are running.

3.5 Management

The last phase of the planning and implementation model is the longest lasting. Managing the solution involves operating the deployed solution and maintaining the application whitelisting architecture, policies, software, and other solution components. Examples of typical actions include:

- Updating the whitelist to include new or updated applications;
- Testing and applying patches to the application whitelisting software;
- Deploying application whitelisting to additional platforms;
- Performing key management duties;
- Adapting policies as requirements change;
- Monitoring the components for operational and security issues;
- Periodically performing testing to ensure that application whitelisting is functioning properly; and
- Performing regular vulnerability assessments.

Organizations should pay particular attention to the ongoing whitelist updates. Although many, if not most, whitelist updates can be automated, administrators should be prepared to make manual updates quickly when needed, in order to identify emerging threats and correct false positives or negatives. Organizations should also monitor any graylists and transfer their entries to whitelists or blacklists, as appropriate.

Appendix A—Security and Compliance Mapping

This appendix provides a mapping to selected standards and guidelines that support using application whitelisting technologies.

NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*[15]

- Control CM-7 (Least Functionality), control enhancement 5 (Authorized Software/Whitelisting): "The organization:

  (a) Identifies [Assignment: organization-defined software programs authorized to execute on the information system];

  (b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and

  (c) Reviews and updates the list of authorized software programs [Assignment: organization-defined frequency]."

***Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*[16]**

- Subcategory PR.IP-1:[17] "A baseline configuration of information technology/industrial control systems is created and maintained." This refers to determining which applications are authorized to be run on each system.
- Subcategory PR.PT-3:[18] "Access to systems and assets is controlled, incorporating the principle of least functionality." This refers to the enforcement of the whitelist established through subcategory PR.IP-1.

***Critical Controls for Effective Cyber Defense, Version 5.1*[19]**

- Critical Control 2: Inventory of Authorized and Unauthorized Software: "Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution."

---

15 http://dx.doi.org/10.6028/NIST.SP.800-53r4

16 http://www.nist.gov/cyberframework/

17 PR.IP stands for Protect: Information Protection Processes and Procedures. This is defined as follows: "Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets."

18 PR.PT stands for Protect: Protective Technology (PT). This is defined as follows: "Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements."

19 http://www.counciloncybersecurity.org/critical-controls/reports/

Appendix B—Applying Application Whitelisting to Mobile Platforms

This appendix discusses considerations involved in applying application whitelisting to mobile platforms (e.g., smartphones, tablets). Typical standalone application whitelisting technologies are generally not available for mobile devices as of this writing. Instead, application whitelisting is achieved through one of two methods: mobile device management (MDM)/mobile application management (MAM) or an enterprise app store.

MDM/MAM

MDM[20] and MAM technologies are suites of security controls for protecting mobile devices from compromises. MDM and MAM technologies often have application whitelisting capabilities built in. Because MDM and MAM technologies are typically centrally managed, they offer a relatively easy way to deploy whitelisting capabilities to mobile devices. However, the disadvantage of relying on application whitelisting in this environment is that mobile applications are constantly changing and new applications are released all the time; it may be prohibitively difficult to maintain application whitelisting solutions with that much flux to be addressed.

Enterprise App Store

An alternative to a client-based application whitelisting technology is an enterprise app store[21]. Many organizations, especially those with MDM deployed to their mobile devices, control the app stores from which their users may download and install apps. This effectively provides a form of application whitelisting, because only those applications that have been approved by the organization for inclusion in the app store may be accessed by the organization's users. There is some maintenance overhead associated with relying on an app store for whitelisting, but it is centralized (approving an app once and posting it to the app store) instead of distributed (configuring thousands of managed mobile devices to recognize the latest apps and app updates).

[20] NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (http://dx.doi.org/10.6028/NIST.SP.800-124r1).

[21] NIST SP 800-163, *Vetting the Security of Mobile Applications* (http://dx.doi.org/10.6028/NIST.SP.800-163).

Appendix C—Acronyms and Abbreviations

Selected acronyms and abbreviations used in the guide are defined below.

FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
ICS	Industrial Control Systems
IT	Information Technology
ITL	Information Technology Laboratory
MAM	Mobile Application Management
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
NSRL	National Software Reference Library
OMB	Office of Management and Budget
OS	Operating System
SIEM	Security Information and Event Management
SP	Special Publication
SSLF	Specialized Security-Limited Functionality

Appendix D—Bibliography

The following publications were used when writing this guide.

- Council on CyberSecurity, *The Critical Controls for Effective Cyber Defense, Version 5.1*, [October 7, 2014], http://www.counciloncybersecurity.org/critical-controls/reports/ [accessed 8/28/2015].
- National Security Agency, *Application Whitelisting Using Software Restriction Policies*, Version 1.1, August 2010, http://www.nsa.gov/ia/_files/os/win2k/application_whitelisting_using_srp.pdf [accessed 8/28/2015].
- National Security Agency, MIT-006FS-2013, *Application Whitelisting [from Top 10 Information Assurance Mitigation Strategies]*, [October 25, 2013], http://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/SlickSheet_ApplicationWhitelisting_Standard.pdf [accessed 8/28/2015].
- NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [accessed 8/28/2015].
- NIST, Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated 1/22/2015), http://dx.doi.org/10.6028/NIST.SP.800-53r4 [accessed 8/28/2015].
- NIST, Special Publication (SP) 800-70 Revision 2, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, February 2011, http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf [accessed 8/28/2015].

ATTACHMENT 7

WEST HIGH SCHOOL

241 North 300 West
Salt Lake City, Utah 84103
Telephone: (801) 578-8500
Fax: (801) 578-8524

Date: _____

To: _____, Student Name & Number

From: _____, West High Administrator

_____, Systems Administrator

_____, Teacher

Guardian/Parent Contact: _____ _____ _____

Name Date Time

Subject: AUP Violation

This memo is to inform you that you are in violation of the West High School Internet Acceptable Use Policy (AUP) Agreement in the following manner:

_____

_____

_____

As a result of your violation, you will receive the following consequence according to the severity and level of your violation:

- ☐ **Level I** - Warning - Classroom Discipline (ex.: non-school related activities, off task)

- ☐ **Level II** – Internet disabled. Parent notification if time off will jeopardize a grade. (ex.: sharing passwords, chatting, playing games or repeat "Level I AUP Violation"). Send form to Assistant Principal to handle.
  - o Temporary privilege removal, 2 weeks or more
  - o Student is required to study and pass AUP test

- ☐ **Level III** – Account disabled, Parent notification (ex.: computer vandalism, hacking, pornography, creating viruses, downloading files or repeat "Level II AUP Violation"). Send form to Assistant Principal to handle.
  - o Suspension (optional)
  - o Permanent privilege removal
  - o Possible criminal charges and consequences

We will be monitoring your computer use throughout the school via a remote view tool on the system network. Please assist us by following our guidelines and reviewing your AUP agreement (available on the SLCSD website (http://www.slc.k12.ut.us/policies/) and select the AUP for Students).

_____ _____
Student Signature Date

_____ _____
Parent Signature Date

_____ _____
Teacher Signature Date

Copy to:

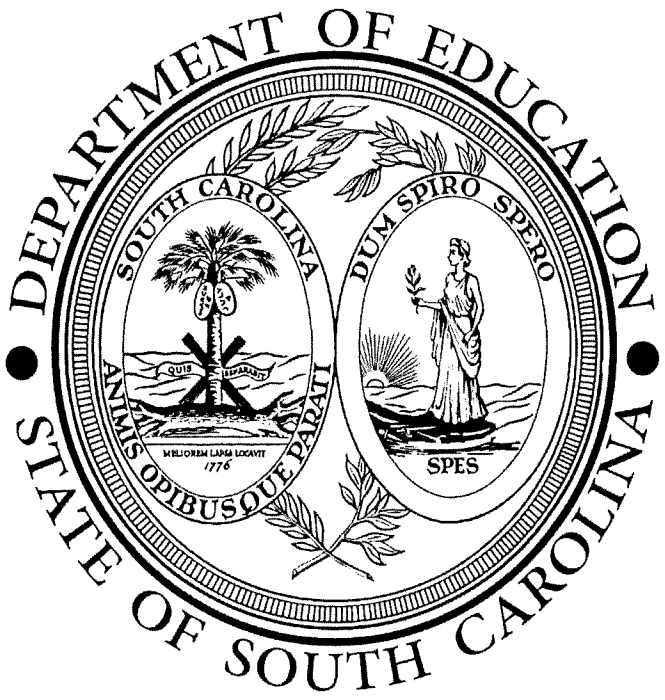
- ☐ Student
- ☐ Teacher
- ☐ Administrator
- ☐ ***Return with parent signature to Teacher***

Discipline Referral Forms should be submitted to the appropriate Assistant Principal listed below (based on the first letter of the student's last name):

- ☐ Mary Margaret Williams, Rm. 208, ext. 257 A thru D
- ☐ Ken DeVries, Rm. 316, ext. 360 E thru K
- ☐ Rick Jaramillo, Rm. 316, ext. 363 L thru Q
- ☐ Gene Bonella, Rm. 316, ext. 319 R thru Z

ATTACHMENT 8

2016 – 2017
FUNDING MANUAL



CHIEF FINANCE OFFICE

REVENUE	**3558**	**READING**
SUBFUND	**358**	**EIA FUND**

Allocation Formula

Funds are distributed on the number of weighted pupil units in each school district in proportion to the statewide weighted pupil units using the 135-day count of the prior year.

Legal References

General Appropriations Act for 2016-2017, Proviso 1A.23

Guidelines

Of the funds appropriated for reading/literacy, the Department of Education, schools, and districts shall ensure that resources are utilized to improve student achievement in reading/literacy. To focus on the importance of early reading and writing skills and to ensure that all students acquire reading/literacy skills by the end of grade 3, fifty percent of the appropriation shall be directed toward acquisition of reading proficiency to include, but not be limited to, strategies in phonemic awareness, phonics, fluency, vocabulary, and comprehension. Forty percent of the appropriation shall be directed toward classroom instruction and intervention to focus on struggling readers and writers in grades 4-8. Ten percent of the appropriation should be directed toward acceleration to provide additional opportunities for deepening and refinement of literacy skills.

Disallowed expenditures include salaries for aides, classroom furniture, and non-instructional equipment, maintenance and computers.

Allowed expenditures include salaries, fringe benefits, consultation services; travel to and from schools and conferences, instructional materials and computers and software used to implement a successful reading program.

The appropriate accounts for **allowed expenditures** are

358-100-100	Instructional Salaries
358-100-200	Instructional Employee Benefits
358-100-300	Instructional Purchased Services
358-100-400	Instructional Supplies and Materials
358-221-100	Improvement of Instruction–Curriculum Development Salaries
358-221-200	Improvement of Instruction–Curriculum Development Employee Benefits
358-221-300	Improvement of Instruction–Curriculum Development Purchases Services

358-221-400	Improvement of Instruction–Curriculum Development Supplies and Materials
358-224-100	Improvement of Instruction In-service and Staff Training Salaries
358-224-200	Improvement of Instruction In-service and Staff Training Employee Benefits
358-224-300	Improvement of Instruction In-service and Staff Training Purchases Services
358-224-400	Improvement of Instruction In-service and Staff Training Supplies and Materials

Because a variety of program activities are permissible, appropriate account numbers will be determined based on services provided and goods delivered in accordance with program guidelines. As a result, the function and object codes displayed above are header codes only and not the detailed function and object account codes which **must be recorded by the district.

Responsible Office: Office of Early Learning and Literacy, Read to Succeed Section
Contact: Cathy Jones Stork, 803-734-0790
E-Mail Address: cjones@ed.sc.gov

REVENUE	**3193**	**EDUCATION LICENSE PLATES**
SUBFUND	**919**	**SPECIAL REVENUE FUND**

Allocation Formula

Funds will be distributed at the end of each quarter based on the number of license plates sold. For each $54 plate sold, $34 will be returned to the district or school chosen by the license plate purchaser. The remaining $20 will be distributed to districts using the ratio of the district's free/reduced lunch count for grades one through three to the statewide free/reduced lunch count for grades one through three of the second preceding year.

Prior year funds may be carried over to the current year.

Legal References

S.C. Code Ann. § 56-3-5010 (2004)

General Appropriations Act for 2016-2017

Guidelines

Public education license plates will be sold statewide at all offices of the Division of Motor Vehicles. Proceeds from the sales will be transferred to the South Carolina Department of Education to distribute to school districts for further distribution to schools chosen by the license plate purchaser. These funds will be used to supplement the technology funds appropriated by the General Assembly and must be used to purchase computer hardware for classroom instruction.

The appropriate accounts for allowed expenditures are

919-100-445	Instruction Technology Software and Supplies
919-100-545	Instruction Technology Equipment and Software

Responsible Office: Office of Finance
Contact: Sue Martinez, 803-734-8145
E-Mail Address: smartine@ed.sc.gov

REVENUE 3630 K–12 TECHNOLOGY

SUBFUND 963 SPECIAL REVENUE FUND

Allocation Formula

Funds will be allocated based on per pupil, based on the previous year's one hundred thirty-five day average daily membership, according to the below calculations: (1) For a school district with a poverty index of less than 75: $35 per ADM; (2) For a school district with a poverty index of at least 75 but no more than 85: $50 per ADM; or (3) For a school district with a poverty index of greater than 85 or a special school with no defined poverty index: $70 per ADM.

Note: The K–12 Technology Partnership Committee's core membership includes a representative from the State Department of Education (SCDE), State Department of Administration's Division of Technology Operations (DTO), Education Oversight Committee, SC State Library, and SCETV. Additional membership includes representatives from private partners representing the telecommunications and Internet-provider communities.

Funding is dependent on decisions made by the K–12 Technology Committee and should be considered non-recurring dollars. This funding is not flexible and must be spent for technology infrastructure as outlined in these guidelines; however, the funds may be carried over into FY 2017–18 should the need arise.

Legal Reference

S.C. Code Ann. § 59-1-525 (2004)

General Appropriations Act for 2016-2017, Proviso 3.6, and Proviso 1.3

Guidelines

Expenditures made with these funds should support the local implementation of the South Carolina Educational Technology Plan, the district technology plan, the district strategic plans and school renewal plans. Purchases should take into account issues projected in long-range plans such as the application of technology to teaching and learning. Funds are to be used for technology infrastructure in the support of educational initiatives such as 1:1 computing, digital learning, high speed connectivity, Wi-Fi enhancement, and online testing. K-12 Technology funds may not be used to supplant existing school district expenditures on technology.

Each district must submit and receive approval of its district technology plan, including technology professional development plans and standards, by the Office of Total Quality Management in the SCDE prior to expenditure of these funds.

Additionally, districts are required to complete an annual online school district technology

inventory site survey for the preceding school year. This survey must be completed for each year in which funds are received or expended, and as prescribed by the SCDE.

If either of these requirements is not currently met by the district, the district is not authorized to expend these funds. Failure to comply with either of these requirements can result in the return of these funds by the district. The SCDE has the right to assess the use of the funds at any time during the fiscal year.

To ensure the maximum impact in each school, the following guiding principles for allowed purchases should be considered. Purchases should

- provide for any hardware, software, or connectivity that is necessary to ensure extended connectivity and use of the dedicated telecommunications lines of the state network;
- supplement but not supplant the existing or projected school and district technology budgets;
- reflect equitable distribution of funds throughout the district;
- reflect planning by a broadly representative committee within the district; and
- match technologies to the local need, considering the fact that all technologies, video equipment, computers, network switches and routers, servers, wireless access hardware, cabling, and others are appropriate uses for these funds.

Responsible Office:	Chief Information Office
Contact:	Don Cantrell, 803-734-3287
E-Mail Address:	dcantrell@ed.sc.gov

ATTACHMENT 9

Internet
Bandwidth Allocation Policy - Version 9
Effective July 1, 2015 (FY 2015-16)

Background

The K-12 Technology Committee has faced many challenges in attempting to meet the goal of economically funding legitimate educational traffic with appropriate and equitable bandwidth allocation for each public school District and Library System in South Carolina. The following updates apply to the Internet Bandwidth Allocation Policy for the state K-12 Schools & Libraries Network members:

A. Internet Bandwidth Allocation Policy for Schools

1. Funded Bandwidth

For FY 2015-16 we will continue to use a "Tiered" approach based on student headcount in each district *(from Free & Reduced Lunch data on the State Department of Education website posted in November before the start of the next July 1 funding year)*. We will move toward a **target** of **UP TO** approximately 10 Kbps per student. For districts with up to 1,500 students, this will result in the district being eligible for a circuit of Up to 150 Mbs. Districts with close to 10,000 students would be eligible for Up to 1 Gbps. Larger districts would have a corresponding eligibility as outlined in the table below. The full amount available to the district is known as the Baseline Maximum Bandwidth. Each has an eligible baseline maximum bandwidth provided at no cost to the district, when approved by the K-12 Technology Initiative Committee or under its delegated authority.

*In an effort to avoid over allocation of bandwidth coverage, Division of Technology (DT) will work with school district technology staff to review usage data when service upgrades are requested. This review process may not result in an immediate increase to the districts baseline maximum tier. DT reserves the right to decrease bandwidth service if periods of over allocation are identified.

The FY 2015-16 Tiers breakdown for School Districts:

Tier	SD Student Headcount	*Baseline Maximum DIA\MIS BW	DIA\MIS Service Cost AT&T/Spirit
1	0 to 1,500	150 Mbs	$ 4,950
2	1,501 to 2,000	200 Mbs	$ 6,050
3	2,001 to 2,500	250 Mbs	$ 6,598
4	2,501 to 3,000	300 Mbs	$ 7,149
5	3,001 to 3,500	350 Mbs	$ 7,423
6	3,501 to 4,000	400 Mbs	$ 7,700
7	4,001 to 4,500	450 Mbs	$ 7,975
8	4,501 to 5,000	500 Mbs	$ 8,250
9	5,001 to 5,500	550 Mbs	$ 9,625
10	5,501 to 6,000	600 Mbs	$10,448
11	6,001 to 7,000	700 Mbs	$11,548
12	7,001 to 8,000	800 Mbs	$12,094
13	8,001 to 9,000	900 Mbs	$12,645
14	9,001 to 10,000	1.0 Gbs	$13,197
15	10,001 to 10,500	1.5 Gbs	$13,866
16	10,501 to 20,000	2.0 Gbs	$14,532
17	20,001 to 25,000	2.5 Gbs	$16,306
18	25,001 to 30,000	3.0 Gbs	$20,942

(CONT.)

19	30,001 to 35,000	3.5 Gbs	$22,252
20	35,501 to 40,000	4.0 Gbs	$23,580
21	40,001 to 45,000	4.5 Gbs	$26,168
22	45,001 to 50,000	5.0 Gbs	$27,489
23	50,001 to 55,000	5.5 Gbs	$29,479
24	55,001 to 60,000	6.0 Gbs	$30,827
25	60,001 to 65,000	6.5 Gbs	$32,148
26	65,001 to 70,000	7.0 Gbs	$33,462
27	70,001 to 75,000	7.5 Gbs	$34,815

Note: *Managed Router Service (CPE) is available to all K-12 Schools & Libraries Network members. Members requesting this service must be willing to pay applicable monthly cost share assessment.*

The tier structure below will be utilized for Special Schools and Career & Technology Centers (CATE).

The FY 2015-16 Tiers breakdown for Special Schools and Career & Technology Centers (CATE):

Tier	SD Student Headcount	Baseline Maximum DIA\MIS BW	DIA\MIS Service Cost AT&T	DIA\MIS Service Cost Spirit (Avg)
1	1 up to 200	30 Mbs	$2,508	$3,141
2	above 201	50 Mbs	$3,111	$3,672

Districts/Special Schools/CATs are eligible for the bandwidth shown above based on student headcount; however, the bandwidth will not be implemented until approved by the K-12 Technology Committee, or by designated authority to the Bandwidth/Security sub-committee, according to the "Bandwidth Qualification Process" described in Section C below. These network members may present their requests or appeal to the K-12 Committee at any time.

B. Internet Bandwidth Allocation Policy for Library Systems

The K-12 Technology Committee faces the same challenge for libraries that it has for schools in the attempt to economically fund legitimate educational traffic with appropriate and equitable bandwidth for each Library System in South Carolina.

1. Funded Bandwidth

For FY 2015-16, DIA/MIS Internet bandwidth for Library Systems will be based on a 10 Mbs minimum funded baseline. DT will allocate funded bandwidth coverage based on usage data. Validation of Internet traffic will also be performed via the use of bandwidth reports provided by SC-ISAC / vendor management tools. Funded Managed Router Service (CPE) can be provided to libraries with 50 Mbs or below Internet Access, when funding is available if requested.

C. Bandwidth Qualification Process

Due to the continued critical budget constraints expected during the 2015-16 fiscal year, the K-12 Technology Committee must confirm that all network members are taking appropriate measures to filter and/or screen traffic so that only legitimate educational traffic is carried before granting approval for any bandwidth above 10 Mbs, regardless of the eligible Tier level. Any network member requesting more bandwidth must demonstrate the true need by undergoing a Security and Traffic Monitoring evaluation to be conducted by the SC Chief Information Security Officer. (See Section C for details.) The cost of this monitoring process will be covered through K-12 funds and at no expense to the network member.

(CONT.)

This will be accomplished as follows:

a. Member provides written request for bandwidth upgrade evaluation to SC State E-Rate Consortium at (k12andERateTeam@admin.sc.gov).

b. State Coordinator submits a traffic monitoring request to the SC Chief Information Security Officer's staff.

c. An Intrusion Detection System (IDS) will be installed on the member's network (if not already in place), either by the SC Chief Information Security Officer staff or the district/library staff. Traffic monitoring will be performed by the SC Chief Security Officer's staff to provide reports on existing bandwidth utilization and recommendations for improvements, if any, to the member. No network changes will be made by the Security Staff unless approved by network member personnel. Full cooperation with the DT Security staff is required for any upgrade.

d. The recommendations and any actions taken will be shared with the E-Rate Coordinator for reporting to the K-12 Technology Committee. The network member will be notified of the date when their request will be reviewed and they are welcome to attend the meeting.

e. The utilization reports and recommendations will be reviewed by the K-12 Technology Committee to determine if the request for additional bandwidth should be approved.

f. The SC State E-Rate Coordinator will notify the network member contact of the Committee's decision and take appropriate action if orders need to be processed.

D. Unfunded Bandwidth

If a network member wants more than the funded baseline bandwidth in their Tier, they will be responsible for the difference in cost of that additional bandwidth. The amount paid by the network member is referred to as the "Cost Share" and is calculated as described in Item 4 below.

4. Cost Share Calculations

The monthly Cost Share is the portion of the Total Cost of the bandwidth above the funded baseline for DIA\MIS service that is not covered by E-Rate funding.

The Cost Share formula is:

Cost of Requested Tier – Cost of Funded Tier = Cost Difference

Cost Difference * District Non-Discount % (100%- District %) = Monthly Cost Share

Example 1 – District A (90%) is in Tier 1 and approved for 10 Mbs DIA & wants 20 Mbs:

Current 20 Mbs cost	$2,535.50 (Spirit Avg for 20 Mbs)
Minus baseline 10 Mbs cost	$1,903.00 (Spirit Avg for 10 Mbs)
=Difference	$ 632.50
Times 10% (100%-90%)	$ 63.25 Monthly Cost Share

(CONT.)

Example 2 – District A (80%) is in Tier 1 and approved for 10 Mbs DIA & wants 20 Mbs:

Current 20 Mbs cost	$2,535.50 (Spirit Avg for 20 Mbs)
Minus baseline 10 Mbs cost	$1,903.00 (Spirit Avg for 10 Mbs)
=Difference	$ 632.50
Times 20% (100%-80%)	$ 126.50 Monthly Cost Share

F. Security and Traffic Monitoring Activities to be performed by the SC Chief Information Security Officer's staff:

- Real-time Monitoring of the K-12 Schools & Libraries Network
  - Network entry point monitoring using an Intrusion Detection System (IDS) on district networks
  - Internal and DMZ monitoring
  - Reporting of most critical security events based on IDS events
  - Notification of critical security events based on SOC monitoring
  - Notification of configuration or hardware issues that may be affecting correct IDS operation
- Real-time visibility / insight over critical assets and bandwidth usage.
- Periodic baseline scans of public-facing IP space.
- Optional service. Some of these services may incur additional costs for hardware, licensing and/or time billed.
  - Security consulting, training, and implementation assistance
  - Security implementation assistance
  - Security policy management, including formulation and review
  - Security system design and planning
  - Network scanning to identify some forms of unauthorized access
  - Incident consulting & law enforcement coordination
  - Assistance with forensic analysis & reporting
  - Web application testing
  - Periodic vulnerability and compliance assessment
  - Caching proxy server installation and host server/reports management. Host server management may be done by network members via their own servers. Where feasible, IDS and proxy may be combined in a transparent in-line configuration for SC-ISAC owned servers.
  - Bandwidth management/improvement consultation

Summary of Previous Policy Revisions

I. **Version 1** - The original document created in 2007 established bandwidth allocations for school districts based on student headcount and placed each district in one of four bandwidth tiers (10 Mbs, 20 Mbs, 50 Mbs or 100 Mbs).

(CONT.)

II. **Version 2** - was approved in 2008 to expand to ten tiers in 10 Mbs increments to provide more flexibility to meet the needs of districts in a more affordable manner. It also added the requirement for Security Monitoring for districts and large libraries before upgrades would be approved.

III. **Version 3** - was approved in August 2009 to update the Internet rates used in Cost Share calculations when the new Direct Internet Access (DIA) contract started July 1, 2009.

IV. **Version 4** - was approved with the following updates effective July 1, 2010. The approved updates in this revision are:

a. Establish new bandwidth baselines

i. School Districts – based on District student headcount with an expanded Tier structure with 10 Megabits (Mbs) increments from 10 Mbs to 200 Mbs.

ii. Library Systems – based on PC count for the Library System.

b. Establish a new Internet Cost Share Formula for schools and libraries

i. Applies to those who want additional bandwidth above what the new baseline provides

ii. Provides Funded Baseline Cost based on the serving Local Exchange Carrier (LEC) rates to avoid penalty in high-cost areas

iii. Uses the individual E-Rate Discount Matrix percentage for each District or Library system to calculate the amount of the Cost Share (rather than the statewide average discount percentage).

c. District/Library System Responsibilities

i. All required E-Rate documents (CIPA and Technology Plans) must be current and on file with the Division of State IT (DSIT) and/or SC Department of Education (SDE).

ii. District/Library must be in good financial standing with DSIT (no past due invoices).

iii. Annual Block 4 Inventory Verification Documents submitted to DSIT by November 15 each year.

1. Any District/Library site not listed on this inventory will be direct billed to the District/Library until the start of the next funding year. (DSIT cannot be reimbursed for sites not listed in the Block 4 section of the statewide E-Rate Applications.)

2. Network members must notify DSIT of site disconnects as soon as possible. Failure to do so could result in a charge to the District/Library for 100% of the ineligible charges paid by DSIT for an inactive location plus any audit re-payments required.

3. For school or library moves or replacements, the state can only fund one circuit; therefore, simultaneous services at both the old site and the new site will only be provided for a maximum of thirty days. After thirty days, the old site will be disconnected or direct billed to the school district or library.

4. Full cooperation with the DSIT Security Staff is required for any Dedicated Internet Access (DIA)/Managed Internet Service (MIS) bandwidth upgrade.

(CONT.)

V. **Version 5** - was approved with no updates effective July 1, 2011.

VI. **Version 6** - was approved and went into effect July 1, 2012. The noted updates in this revision are:

a. **District/Library System Responsibilities**
   i. Modify title, and statements to include the words "School" and "CATE".

   ii. Add the following statements regarding CIPA compliance requirements to remain an active member of the K-12 Schools & Libraries Network.
      1. All schools/network members residing on the K-12 Schools & Libraries Network must be 100% compliant with the "Protecting Children in the 21st Century Act" by July 1, 2012 as required by the FCC E-Rate Program rules.

      2. Any school/district/library that is noncompliant with E-Rate CIPA rules may be removed from the K-12 Schools & Libraries Network. This will result in direct billing for services rendered.

      3. Request to be returned to the network will require proof of compliance before approval can be granted.

b. **Internet Bandwidth Allocation Policy for Schools**
   i. Add new separate Tier Structure for School Districts
   ii. Revise current 10 Mbs tier structure (tiers eliminated)
   iii. Increase minimum bandwidth baseline to 100 Mbs for School Districts
   iv. Include Managed Internet Service (MIS) to service description

c. **Security and Traffic Monitoring Activities to be performed by the SC Chief Security Officer's staff**
   i. Updated statements added to this section of the policy.

VII. **Version 7**- Proposed policy revisions to go into effect July 1, FY 2013-14:
   i. Revise "Background" statement
   ii. Remove current 100 Mbs baseline, six tier structure for Districts
   iii. Add new target 10 kbps per student baseline information for Districts
   iv. Add a 29 tier structure for Districts
   v. Add statement:" In an effort to avoid over allocation of bandwidth coverage, DSIT will work with school district technology staff to review usage data when service upgrades are requested. This review process may not result in an immediate increase to the districts baseline maximum tier. DSIT reserves the right to decrease bandwidth service if periods of over allocation are identified."
   vi. Updated "DIA\MIS Service Cost (AT&T\Spirit (Avg) Cost" charts
   vii. Relocated sections "Bandwidth Qualification Process" and "Internet Bandwidth Allocation Policy for Library Systems"
   viii. Changed "schools and libraries" and "district/library" to "network member"
   ix. Corrected position title "SC Chief **Information** Security Officer"
   x. Add Note: Managed Router Service (CPE) is available to all K-12 Schools & Network members. Any member can request this service must be willing to pay applicable monthly cost share assessment

(CONT.)

xi. Revise "B. Internet Bandwidth Allocation Policy for Library Systems"
    1. Remove all references to the use of Internet access enabled personal computers (PCs) counts as a determining factor for eligible bandwidth tiers. Tier table removed.

xii. Add statement: "Validation of Internet traffic will also be performed via the use of bandwidth reports provided by SC-ISAC / vendor management tools. Funded Managed Router Service (CPE) will be provided to libraries with 50 Mbs or below Internet Access, when funding is available if required."

xiii. Add Note: Library Systems minimum funded bandwidth baseline will be 10 Mbs.

VIII. **Version 8** – Approved policy revisions to go into effect July 1, FY 2014-15:
- i. Revise the tier structure for Special Schools and Career & Technology Centers (CATE)
    1. Modified Tier table to include two levels (13 tiers removed)
- ii. Remove the following statement: "No "grandfather clause" will apply under this policy; therefore, sites that already have more bandwidth than they are eligible for under the 2012 Internet Policy will begin paying the appropriate Cost Share on July 1, FY 2013-14."

IX. **Version 9** – Approved policy revisions to go into effect July 1, FY 2015-16
- i. section "A. Internet Bandwidth Allocation Policy for Schools"
    1. "Funded Bandwidth" section wording "1,000"students changed to "1,500"students, "100"Mbs changed to "150"Mbs
    2. Revise the funded bandwidth tier chart section
        a. Tier "1" and "2" remove. Modify Tier "3" to reference (0 to 1,500 students, 150 Mbps) and reassign this level Tier "1"
    3. Update service cost for tiers to reflect accurate/new rates.
    4. Update "Unfunded Bandwidth" section 4 "Cost Share Calculations", Example 1 and Example 2 to reflect current pricing per reference bandwidth speed. Removed the verbiage "(an increase is approved by the K-12 Technology Committee"
    5. Change all "FY 2014-15" references to read "FY 2015-16"
    6. Change all "DSIT" references to read "DT" (Division of Technology)
    7. Other revisions: Update the Bandwidth Allocation Policy version 6 statements
        a. "District/Library System Responsibilities" statement to change all "DSIT" references to read "DT"
        b. **Change:** "All required E-Rate documents (CIPA and Technology Plans) must be current and on file with the Division of State IT (DSIT) and/or SC Department of Education (SDE)." **To:** "All required E-Rate documents and a current approved Technology Plan Letter must be on file with the Division of Technology (DT) and/or SC Department of Education, State Library."