



# Dinwiddie County Public Schools

P.O. Box 7, 14016 Boydton Plank Road, Dinwiddie, Virginia 23841  
804-469-4190 ☎ Fax: 804-469-4197

*A Place to Learn... A Place to Grow... A Place to Belong*

# 2016 - 2018

## Educational Technology Plan Addendum

## Technology Plan Committee Members



### **Technology Support**

Shawanna Hill,  
Technology  
Support Specialist -  
Mobile

Toni Wynn,  
Assistant Director  
of Technology

Timothy Ampy,  
Director of  
Technology



### **Instructional Technology**

Christine Bastaich,  
Instructional  
Technology  
Resource Teacher

Christie Clarke,  
Director of  
Instructional  
Technology



### **Parent Representative**

Kathy McCoun



### **School Administration**

Amber Brown,  
Assistant Principal -  
Dinwiddie High  
School

Alfred Cappellanti,  
Principal - Dinwiddie  
Middle School

Davis Roberts,  
Principal - Dinwiddie  
Elementary School



### **Central Office**

Dr. Kari Weston,  
Assistant  
Superintendent of  
Instruction

Sharon Yates, Director  
of Secondary  
Education and Career  
& Technical Education



### **Classroom Representatives**

Danielle Hawkins,  
Media Specialist –  
Sunnyside Elementary  
School

Randy Bullock,  
Teacher – Dinwiddie  
High School

## *Table of Contents*

<b>EXECUTIVE SUMMARY</b>	<b>4</b>
<b>TECHNOLOGY A DEFINITION</b>	<b>5</b>
<b>VISION STATEMENT</b>	<b>5</b>
<b>MISSION STATEMENT</b>	<b>5</b>
<b>HORIZONS</b>	<b>5</b>
<b>CURRENT STATUS</b>	<b>6</b>
<b>UPDATED ACCOMPLISHMENTS</b>	<b>7</b>
<b>PROJECTS FOR 2015 - 2018</b>	<b>9</b>
<b>NEEDS ASSESSMENT</b>	<b>10</b>
<b>VDOE TECHNOLOGY PLAN GOALS</b>	<b>12</b>
<b>APPENDICES</b>	<b>29</b>

## **EXECUTIVE SUMMARY**

The development goal of the Dinwiddie County Public Schools (DCPS) Technology Planning Committee is to create a technology plan that will align with both our local strategic action plan as well as the Educational Technology Plan for Virginia while also complying with the requirements of the “No Child Left Behind” Act. Additionally, this plan will assist in identifying the resources and strategies that enable the most effective uses of technology in our schools. Our Committee of stakeholders expended a considerable amount of time reviewing the State Educational Technology Plan in conjunction with our local Technology Plan and Progress Report as well as existing DCPS policies and guidelines in preparation for the new Technology Plan. Dinwiddie County Public Schools’ information technology has become an essential tool of education, research, planning and daily life. Information technology has become a keystone for students’ education and professional careers, but it also has opened up an exciting range of creative, scholarly, and entrepreneurial opportunities for students and faculty alike. Our division has provided significant resources toward fostering effective uses of information technology in the advancement of education. Dinwiddie County Public Schools was awarded the Division Leadership Award by the Southside Virginia Regional Technology Consortium which is composed of thirty school divisions. The criteria for this award was based upon the capability of a school division to completely embrace information technology, with purpose and imagination, to maintain its place among the area’s leading divisions and to provide the finest education for its students. Dinwiddie received this award in 2008. The goal for the 21<sup>st</sup> century should be nothing less than to position the division as a leader in using information technology. To achieve this goal, information technology must become a pervasive and transparent part of the lives of students, faculty and staff. Information technology is pervasive when it is available as a matter of course to everyone; it is transparent when information and applications are available without delays or limitations imposed by hardware, software, or technical support. Users must experience technology as seamlessly integrated into their activities. Investments in providing pervasive computer access will earn far greater dividends when hardware is more mobile, when user interfaces operate more intuitively, when search engines return more meaningful results, and when information can be used easily for multiple purposes. This plan presents specific goals and recommendations to achieve and maintain excellence in information technology in support of the missions of the division and the guidelines of the “Elementary and Secondary Education Act”. These goals are as follows...

- Teachers will integrate technology concepts and practices in the classroom
- IT staff will stay current with emerging technologies and professional development
- All teachers will integrate Internet Safety lessons throughout the curricula
- Parental communication will increase through various technology mediums
- A replacement schedule for all technology equipment will be implemented on a four year cycle
- All classrooms will be connected to the WAN via high speed networks to improve Internet access
- A funding schedule for replacement equipment will be devised and supported by the budget process
- Software that supports classroom learning and VA SOL standards will be purchased and implemented
- Additional means of funding will be sought after with grant writing to supplement not supplant the annual local technology funding
- Progress of the plan will be evaluated annually
- Reduce paper usage and promote green technology
- Administrative staff provided with anytime, anywhere access to division critical data
- Seek cost savings technologies where applicable

## VISION

- Dinwiddie County Public Schools functions more efficiently and assists individual schools as they utilize technology to improve the teaching and learning experience for their students.

## MISSION

- The mission of Dinwiddie County Public Schools is to provide each student the opportunity to become a productive citizen, engaging the entire community in the educational needs of our children. The mission of the DCPS Technology Department is to further advance the overall mission of the school system by using technology to improve the teaching and learning experience for our students. We truly believe that technology should be integrated fully in every area of our school division to enable each student, teacher and staff to reach their educational goals in the 21st century.

## HORIZONS

- We believe that connecting all of our schools with gigabit fiber has enabled us to expand our network and provide a framework for future growth of both our school division and our community at-large. **We aspire to provide learning opportunities with anytime, anywhere access to mission-critical instructional, administrative and network information as we move forward with 21<sup>st</sup> century educational technology in the creation of digital learning environments.**

## ***TECHNOLOGY, A DEFINITION***

Science used to solve practical problems. Technology includes the use of materials, tools, techniques, and sources of power to make life easier or more pleasant and work more productive. Whereas science is concerned with how and why things happen, technology focuses on making things happen. Technology for the purposes of this technology plan therefore may include but not be limited to the following: software, hardware, data, Internet/Intranet, computers, servers, monitors, printers, switches, routers, access points, probe ware, TVs, LCD projectors, media players/recorders, analog/VoIP phones, cell phones, iPods, flash drives, calculators, radios, digital cameras, video cameras, PDAs (personal digital assistant), blogs and wikis.

## ***CURRENT STATUS***

Numerous things have changed in Dinwiddie County Public Schools in regards to technology since our last Technology Plan. All schools are presently connected to the Internet by the use of gigabit fiber at each school site, as well as the administrative office complex, transportation and maintenance site. All locations are connected to the Internet through a 50-megabit Internet pipe at our Demarc site. Additionally, all of our schools are currently E-Sol certified; our entire school division has wireless-G at all locations which were installed completely in-house by the DCPS technology department. Another successful strategy that we are currently employing is the implementation of a new state-recommended web-based Student Information System. All of our teacher laptops have been replaced at both the elementary and secondary level. All schools now have gigabit core switches which have improved the over-all bandwidth of our network infrastructure. Each school's existing capability is at least a 1000 megabits switched network. Every elementary school has at least three computers or three virtual desktops in every classroom, one computer lab and three laptop carts. The middle, junior high and senior high schools have four, five and nine labs or laptop carts, respectively, at each location. At the present time we still have some server-based programs, however, we are gradually transitioning towards more web-based programs in order to provide anytime, anywhere access to our students, parents, administrators, teachers and staff. We have also opened a new professional development center that has internet access and encompasses a conference room, training rooms and a computer lab.

Currently each teacher has a laptop available for use in our school division. Staff development institutes have included hands-on activities and work sessions which have generated positive discussions and a heightened awareness of how students can best benefit from technology integration. In a peer environment our administrators have felt more comfortable asking questions about the true nature and practical implications of issues such as project-based learning and constructivist principles.

## **UPDATED ACCOMPLISHMENTS FROM 2005 – 2011**

- Installed Gigabit fiber at all school locations
- Upgraded all school LANs to 1000 megabits
- Transitioned to an Active Directory environment division-wide
- Completed E-SOL certification requirements at all school sites
- Increased Internet Demarc from 45 to 50 megabits
- Installed WLAN 802.11G division-wide
- Added 3-5 new virtual desktops in each elementary school classroom
- Replaced all teacher laptops at both the elementary and secondary level
- Added 5 (24-count) laptop carts division-wide
- Implemented a web-based IT Help Desk
- Rolled out a web-based Employee Portal (KeyNet)
- Transitioned to a web-based Student Information System (Infinite Campus) with parent and student portals
- Completed implementation of a web-based library management system (Destiny) at all school sites
- Added division-wide Blogging servers for Staff and Students
- Instituted a Software Approval committee to help review and evaluate software per curriculum goals
- Added 5 new computer labs(1 at the high school, 1 at the junior high school and 3 at the middle school)
- Transitioned to a division-wide mass notification system
- Replaced all old CRT monitors at the middle and junior high schools with 19" LCD monitors
- Upgraded memory at both the school sites and the Central Office
- Added a centralized web filter proxy with heightened security features
- Added networked digital copiers division-wide
- Revised the division Acceptable Use Policy per compliancy regulations set forth by the state legislature

## **UPDATED ACCOMPLISHMENTS FROM 2011 – 2014**

- Replaced all Elementary Schools' teacher laptops
- Replaced 5 computer labs at Dinwiddie High School

- Replaced 6 computer labs at Dinwiddie Middle school
- Replaced all Administrators' computers with Windows 7 desktops
- Replaced many of the division's mobile computer carts
- Upgraded mass notification system to Blackboard Connect 5
- Revamped division and school websites
- Upgraded division Firewall
- Added AESOP absence management software
- Added Nooks, iPads and iPad Minis to all schools
- Upgraded Internet Demarc to 100 Megabits
- Installed and configured new division Proxy
- Updated school bookkeeping software to a newer, web-based product (TRA)
- Implemented Secondary Assessment Software (ROSworks)
- Replaced all Elementary Schools' lab computers
- Deployed new Textbook Manager and Asset Manager programs (Follett Destiny)
- Upgraded Dinwiddie Middle School's core infrastructure
- Converted old student records to digital format via Cloud storage

## **UPDATED ACCOMPLISHMENTS 2014 – 2015**

- Provided Tablet Devices Dinwiddie High School Students in grades 9 – 10
- Provided Tablet Devices in mobile carts to Dinwiddie Middle School Students
- Upgraded Internet Demarc to 250 Megabits
- Deployed newer School Nutrition Software with Online Payment Module (Meals Plus)
- Replaced old telephone systems (POTS) in some Elementary schools with new VoIP system
- Transitioned to Google Apps for Education (GAFE)
- Issued email accounts to students in grades 6 – 12
- Replaced all Secondary Schools' teacher laptops
- Migrated to new Digital Copiers (Ricoh)
- Deployed Assessment programs (Interactive Achievement K – 8; ROSworks 9 – 12 )
- Added new security system division-wide
- Installed new application servers at secondary schools
- Installed new e-mail archiving appliance



- Created new GED lab for training and testing
- Continued to upgrade WAN core infrastructure
- Created Division and School Applications
- Added IP clocks to Elementary and High Schools
- Added a Technology Support Staff for mobile devices

## **PROJECTS 2015 – 2018**

- Add additional Instructional Technology Resource Teachers
- Add additional Technology Support Staff
- Upgrade WAN core infrastructure and Demarc as needed
- Upgrade wireless network division-wide to new 5GHz speed
- Provide Tablet Devices to incoming 9<sup>th</sup> grade students (students in grades 9 – 11 have tablets)
- Provide Tablet Devices (2 carts) for use by Middle School Students
- Install Web Caching Appliance on the WAN
- Replace all Elementary school main servers
- Continue implementation of Interactive Achievement (K-12)
- Deploy Enterprise Mobile Device Management and Security System
- Start division-wide Credit Recovery program
- Create Student Technology Support Team at secondary schools
- Implement annual Technology/STEM Camps
- Provide additional Technology-enriched classes to students (K-12)
- Increase online and distance learning opportunities for students
- Replace old telephone systems (POTS) at remaining Elementary schools with new VoIP systems
- Replace all old network cabling infrastructure at the Middle School
- Create a more robust disaster recovery network
- Deploy virtual storage and Servers to increase division-wide network storage capacity
- Replace Elementary School teacher laptops

## **NEEDS ASSESSMENT**

### **Technology Planning Committee**

The technology planning committee started June 10, 2010 by reviewing the old plan and the new technology goals stated in the Educational Technology Plan for Virginia. Since that time we have been gathering information from staff, teachers, students, parents and many other sources. The committee also met on the following dates: August 10<sup>th</sup>, 12<sup>th</sup>, 19<sup>th</sup>; October 13<sup>th</sup>; November 3<sup>rd</sup> and November 15<sup>th</sup>. An online survey was developed by the committee and issued out on November 4, 2010 to all teachers in the division in order to obtain feedback from them in the areas of technology integration and support. The data from this survey was analyzed and discussed during the November 15<sup>th</sup> meeting of the technology committee. As a result of that analysis, it was further established that getting the right technology in the hands of our teachers, students and staff would aid in reaching our goal of creating anytime, anywhere access digital learning environments. In October 2015, the Technology Committee (in part) reconvened to both identify current needs as well as to draft the 2015-2018 addendum to this original plan.

### **Annual Technology Planning Meetings**

The technology director meets each year with the principals of each school to discuss technology needs in their respective buildings. The principal generally receives this type of information from polling their teachers and staff. The technology director also meets with the school board administrative staff in order to ascertain exactly what is needed to keep their respective departments successful and progressing forward. There are bi-monthly meetings of the entire technology team which consists of the technology support staff, the ITRTs, the instructional technology director, the assistant director of technology and the director of technology. Both the support and instructional sides work closely together to ensure technology is present and available to be integrated into the classroom at all levels. Our Software Approval committee meets bi-monthly as well and strives to research and assess potential instructional software and how it can further prepare our students, teachers, and staff for the changes of the future. The Technology Planning Committee will meet quarterly to strategize and prioritize existing goals and objectives in addition to developing future initiatives for implementation.

### **Curriculum Integration**

All DCPS teachers have laptop computers for instructional use. Teachers are provided training and ongoing technical support. The laptops are used to support classroom instruction on a regular basis.

Laptop carts are available at all levels. Through observation and usage data, it was found that teachers who did not attend small group instruction and integration training were far less likely to use laptop carts. The ITRTs continue to focus on how constructivist learning can positively impact students. The ITRTs collaborate with classroom teachers for technology integration. We believe that we can foster an environment for student and teacher success over time by having the appropriate technology integration staff onsite, along with strong building leadership.

Thousands of lessons and template activities have been developed by the ITRTs which are correlated to specific grade level/content SOLs and the local pacing guide. These have been uploaded to a shared area

of the DCPS intranet for use by all instructional staff for either in-class and/or lab related activities. This is an ongoing project and lessons are evaluated regularly for effectiveness. A recent review of all activities for grades K-5 was completed in December 2015.

Technology staff development offerings continue to be in great demand. Teachers are most interested in practical project-based classes as opposed to process or software how-to-courses. Hundreds of workshops have been offered to teachers since January 2007.

## **Internet Safety**

House Bill 58, introduced by Delegate William H. Fralin, Jr. and passed by the 2006 General Assembly, requires that school divisions' acceptable use policies "include a component on Internet safety for students that is integrated in a division's instructional program." The legislation also requires the Superintendent of Public Instruction to issue guidelines to school divisions regarding instructional programs related to Internet safety.

The 2006 legislation requires divisions to integrate the new Internet safety component within the curriculum. School divisions need to design the program specifically to each grade level. Students will learn about Internet safety from kindergarten through high school graduation, acquiring new skills each year while being reminded of previous lessons. All instructors, not just library media specialists or computer-lab teachers, will teach Internet safety and take every opportunity to warn of potential dangers and model safe and appropriate Internet use.

## **Educational Applications**

Currently we make use of the following software applications.

- Desktop – Windows 7, Office 2007, Office 2010, Office 2013, Inspiration (6-12), Kidspiration, Follett Circulation Plus, Kaspersky Antivirus 10.0, Hyperstudio and TimeLiner
- Web Applications – Google Apps, Infinite Campus–Student Information System, Student +Parent Portals, Destiny - Library System, BlackBoard Connect 5 - Mass Communication System, Gale Group – Online Library Subscription, World Book Online, SIRS – Online Library Research Database, Workkeys - Student Assessment program, Study Island and Interactive Achievement
- Network Applications – TestNav
- Administrative Applications –Infinite Campus, CanDo Online Competency Evaluation, VersaTrans, Fleet Vision, Meals Plus, BlackBoard Connect 5, Online Payment System for parents
- Probe ware, Robotics

## **Infrastructure**

Ninety-five percent of the Dinwiddie County Public Schools' infrastructure of switches, laptops, desktops and servers is the Hewlett-Packard brand. Our network is a switched gigabit. Since much of the newer technology is of the small size and wireless; we shall also continue to upgrade our wireless network so as

to stay current and efficient in daily operations. We plan to upgrade even more by making 10 Gigabit the standard though-out the division. Network security and intrusion prevention have also become a more important issue in the daily operation of technology use at all levels.

## **Data Collection and Data Analysis**

The collection of data and reporting to the state and other agencies has greatly improved with the addition of the SIF server and agents that are currently installed. We expect to acquire additional SIF agents as the demands and requirements of both state and federal reporting increase.

## **VDOE TECHNOLOGY PLAN GOALS**

The 2015-2017 Addendum to the Educational Technology Plan for Virginia: 2010-2015 imparts state-level goals and objectives grounded in a foundation of research and based on identified needs (see Appendix B). School divisions must develop locally appropriate strategies and measures that address these statewide goals and objectives while, at the same time, leveraging their unique strengths and minimizing the gaps between promise and practice. Beyond the goals and objectives of the state's plan, division technology committees may create effective plans by adding goals and objectives that support division missions and visions.

Virginia school divisions are practiced in the art and science of good planning procedures. Division technology plans need to follow these procedures, reflect state and local goals, and be useful to all stakeholders. With an increased emphasis on supportive data collection, divisions also must collect appropriate and useful information during the evaluation phase of the planning cycle.

### **Goal 1**

Provide a safe, flexible, and effective learning environment for all students

#### **Objective 1.1**

Provide the technical infrastructure necessary to support formal and informal learning environments.

#### **Objective 1.2**

Provide the human infrastructure necessary to support formal and informal learning environments.

#### **Objective 1.3**

Develop sound policies and procedures for the acquisition and management of technologies.

### **Goal 2**

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

#### **Objective 2.1**

Deliver appropriate, rigorous, and challenging technology-enhanced curricula to support formal and informal learning experiences.

### **Objective 2.2**

Provide resources to support personalized learning for all students.

## **Goal 3**

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

### **Objective 3.1**

Provide resources and applications that encourage creativity, collaboration, and problem solving.

### **Objective 3.2**

Develop and evaluate technology policies to effectively balance the need for instructional innovation with safety and security.

## **Goal 4**

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

### **Objective 4.1**

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

### **Objective 4.2**

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

## **Goal 5**

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

### **Objective 5.1**

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

### **Objective 5.2**

Promote the use of technology to support the design and implementation of next generation assessments.

This Page Intentionally Left Blank.

## Environment

<b>Goal 1: Provide a safe, flexible, and effective learning environment for all students.</b>					
<b>Objective</b>	<b>Strategy</b>	<b>Responsible Party</b>	<b>Timeline</b>	<b>Evaluation</b>	<b>Estimated Cost</b>
1. Deliver appropriate and challenging curricula through face-to-face, blended, and virtual learning environments.	a. Increase the use of online courseware products to facilitate credit-recovery as well as the addition of high-tech courses to our secondary curriculum.	Director of Technology, Director of Secondary Education, Director of Elementary Education, Guidance Department, Principals	2015-2016	Student Reports (report cards, transcripts), Graduation/Drop-Out Reports	\$15,000 Annually
	b. Preserve existing and establish new agreements/partnerships with local colleges and universities to sustain dual enrollment course offerings.	Director of Secondary Education, Director of Student Services & Assessments, Guidance Department	Annually	Review & Revise Memorandum of Agreement/Memorandum of Understanding w/local colleges & universities	In-House

## Environment

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
2. Provide the technical and human infrastructure necessary to support real, blended, and virtual learning environments.	a. Upgrade the network back-bone to 1 GB and 10 GB where deemed necessary.	Director of Technology, IT Staff	Annually	Network Bandwidth Testing & Reports	\$30,000 Annually For 3 Years
	b. Upgrade wireless access points to type new 5GHz at all sites.	Director of Technology, IT Staff	2015 - 2016	Wireless Data Management Reports	\$15,000 Annually For 3 Years
	c. Review current technical and instructional staffing needs and make adjustments as needed.	Director of Technology, Director of Instructional Technology, School Board	Annually (During Budget Planning)	Help Desk Reports, Activities Logs, Surveys	In-House
3. Provide high-quality professional development to help educators create, maintain, and work in a variety of learner-centered environments.	a. Present locally-designed staff development institutes on instructional technology applications, strategies and best practices.	Director of Technology, Director of Instructional Technology, Central Office Instructional Team, ITRTs	Annually	Surveys, Training Evaluations	In-House
	b. Present technical training on fundamental skills, knowledge and best practices to teachers, staff and administrators.	Director of Technology, IT Staff	Annually As Needed	Surveys, Training Evaluations	In-House



## Engagement

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

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
1. Support innovative professional development practices that promote strategic growth for all educators and collaboration with other educators, content experts, and students.	a. Continue participation in consortium-based and regional-based training opportunities.	Director of Technology, Director of Instructional Technology, Central Office Instructional Team	Annually	Review memberships and subscriptions	In-House
	b. Attend conferences, meetings, workshops and seminars on best practices and integration strategies.	Director of Technology, Director of Instructional Technology, Central Office Instructional Team	Annually	Conference/Training summaries and presentations	\$25,000 Annually
2. Actualize the ability of technology to individualize learning and provide equitable opportunities for all learners.	a. Install/replace interactive whiteboards in all classrooms across all grade levels.	Director of Technology, Director of Instructional Technology, Central Office Instructional Team	Annually	Purchase Orders and Invoices	\$30,000 Annually For 5 Years

## Engagement

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
	b. Increase use of portable technologies, i.e., iPods, iPads, Nooks, netbooks and e-readers into varied learning environments to enrich instruction.	Director of Technology, IT Staff, Director of Instructional Technology	Annually	Surveys, Observations, Technology Usage Reports	\$30,000 Annually
3. Facilitate the implementation of high-quality Internet safety programs in schools.	a. Educate students on Internet safety and etiquette by utilizing in-class presentations and demonstrations.	Director of Technology, Director of Instructional Technology, ITRTs, Principals	Annually As Needed	Surveys, Observations	In-House
	b. Educate teachers, staff and administrators on Internet safety and etiquette by utilizing e-mail, workshops and in-services.	Director of Technology, Director of Instructional Technology, ITRTs, Principals	Annually As Needed	Surveys, Observations	In-House

## Engagement

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
	c. Educate parents, families and communities on Internet safety and etiquette by utilizing e-mail, brochures, newsletters and mass media outlets.	Director of Technology, Director of Instructional Technology, ITRTs, Principals	Annually As Needed	Surveys, Observations	In-House

## Application

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

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
1. Provide and support professional development that increases the capacity of teachers to design and facilitate meaningful learning experiences, thereby encouraging students to create, problem-solve, communicate, collaborate, and use real-world skills by applying technology purposefully.	a. Research and present training on best practices and instructional strategy development.	Director of Instructional Technology, Central Office Instructional Team	Annually	Surveys, Observations	\$5,000 Annually
	b. Promote sharing and collaboration across content and curricular areas regarding innovative technologies and curriculum integration.	Director of Technology, Director of Instructional Technology, Central Office Instructional Team, ITRTs, IT Staff	Annually	Usage Reports, Surveys, Observations	\$10,000 One-Time Cost
2. Ensure that students, teachers, and administrators are ICT literate.	a. Present regular technology camps and expos featuring innovative technologies and practices.	Director of Technology, Director of Instructional Technology, IT Staff, ITRTs, Central Office Instructional Team	Annually	Surveys	\$15,000 Annually

## Application

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
	b. Provide opportunities for student collaboration by using e-mail, social networking sites, wikis and blogs.	Director of Technology, IT Staff, Coordinator of Technology, ITRTs	Annually	Usage Reports	\$10,000 Annually
	c. Provide opportunities for teacher and administrator collaboration by using e-mail, social networking sites, wikis, blogs and instructor web sites.	Director of Technology, IT Staff, Coordinator of Technology, ITRTs	Annually	Usage Reports	\$1,000 Annually
	d. Utilize podcasting, video-conferencing/video-casting and other media for communication and collaboration.	Director of Instructional Technology, ITRTs, IT Staff	Annually	Usage Reports, Surveys	\$10,000 Annually
3. Implement technology-based formative assessments that produce further growth in content knowledge and skills development.	a. Employ online tools like Interactive Achievement and Study Island across grade levels to supplement instruction and assess learning.	Director of Technology, Director of Instructional Technology, IT Staff, ITRTs, Central Office Instructional Team	Annually	Usage Reports	\$30,000 Annually

## Application

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
	b. Utilize the CanDo application at the high school level to assess knowledge, competencies and skills obtained.	Director of Secondary Education, IT Staff	Annually	Usage Reports	\$1,000 Annually
	c. Utilize the WorkKeys application at the high school level to assess knowledge and initiate career-readiness.	Director of Secondary Education, IT Staff	Annually	Usage Reports	In-House
	d. Employ Interactive Achievement across grade levels to assess knowledge and direct instruction.	Central Office Instructional Team, IT Staff	Annually	Usage Reports	\$45,000 Annually

## Tools

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

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
1. Provide resources and support to ensure that every student has access to a personal computing device.	a. Continue to deploy portable technologies, i.e., iPods, iPads, Nooks, netbooks and e-readers into varied learning environments to enrich instruction.	Director of Technology, Director of Instructional Technology, ITRTs, Teachers	Annually	Surveys, Observations	\$25,000 Annually
2. Provide technical and pedagogical support to ensure that students, teachers, and administrators can effectively access and use technology tools.	a. Present training on best practices of curriculum integration of advanced technologies and other tech tools.	Director of Instructional Technology, ITRTs, IT Staff	Annually	Surveys, Observations	In-House
	b. Continue to add newer technology devices to classrooms across all grade levels.	Director of Technology, IT Staff	Annually	Purchase Orders and Invoices	\$25,000 Annually

## Tools

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
	c. Refresh lab computers every 4 years.	Director of Technology, IT Staff	Every 4 years	Purchase Orders and Invoices	\$75,000 Annually For 4 years
	d. Refresh laptops issued to teachers and staff every 4 years.	Director of Technology, IT Staff	Every 4 years	Purchase Orders and Invoices	\$50,000 Annually For 4 years
	e. Continue to implement a web-based technology help desk to capture and resolve all technology-related help requests.	Director of Technology, IT Staff	Annually	Usage Reports, Surveys	\$1,000 Annually Maintenance Cost
3. Identify and disseminate information and resources that assist educators in selecting authentic and appropriate tools for all grade levels and curricular areas.	a. Form a technology advisory council/committee to research new solutions and recommend pilot technology projects.	Director of Technology/Technology Manager	2015 - 2016	Meeting Summaries, Surveys, Observations, Usage Reports	In-House
	b. Conduct regular meetings with administrators to discuss relevant technology topics.	Director of Technology, IT Staff	Annually As Needed	Discussion Summaries	In-House



## Tools

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
	c. Recommend webinars, conferences, workshops and in-services on emerging and advanced educational technologies.	Director of Technology, Director of Instructional Technology, IT Staff, ITRTs, Central Office Instructional Team, Principals	Annually As Needed	Presentations, In-services	\$15,000 Annually

## Results

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

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
1. Use data to inform and adjust technical, pedagogical, and financial support.	a. Compile and analyze results from existing benchmarking assessment tools.	Central Office Instructional Team, Principals	Annually	Data Reports	In-House
	b. Collect feedback from the different educational dynamics – students, parents, teachers, staff and administrators.	Central Office Instructional Team, Principals, Teachers	Annually	Surveys, Data Reports	In-House
	c. Examine the results of technology usage reports.	Director of Technology, Director of Instructional Technology	Annually	Data Reports	In-House
2. Provide support to help teachers disaggregate, interpret, and use data to plan, improve, and differentiate instruction.	a. Conduct locally designed staff development institutes focusing on the characteristics of a data culture.	Director of Technology, Director of Instructional Technology, ITRTs, IT Staff	Annually	Surveys, Observations	In-House
	b. Promote attendance at workshops, seminars and conferences geared toward compiling and analyzing educational data.	Central Office Instructional Team, Director of Instructional Technology, ITRTs, IT Staff	Annually	Surveys, Observations	In-House

## Results

Objective	Strategy	Responsible Party	Timeline	Evaluation	Estimated Cost
3. Promote the use of technology to inform the design and implementation of next-generation standardized assessments.	a. Increase the use of Interactive Achievement across all grade levels for benchmark assessments and enrichment activities.	Central Office Instructional Team, IT Staff	Annually	Usage Reports	\$45,000 Annually
	b. Continue the conversion of paper-and-pencil tests to digital and online formats.	Central Office Instructional Team, IT Staff	2015 - 2016	Technology Usage Reports	In-House
	c. Research and pilot various assessment tools/applications geared toward improving student achievement.	Central Office Instructional Team, IT Staff	Annually As Needed	Surveys, Observations, Usage Reports	\$15,000 Annually

This Page Intentionally Left Blank.

## ***PARTNERSHIPS***

These partners assist the schools in meeting several technology goals. Continuation of and the formation of new partnerships are ongoing. The following is a list of current partnerships that have been formed:

Southside Virginia Regional Technology Consortium (SVRTC)

John Tyler College PEER Consortium

Institute For Teaching Through Technology & Innovative Practices (ITTIP) - An outreach of Longwood University

Electronic Systems Integration (ESI)

Uptime Solutions

## ***APPENDICES***

Acceptable Use Policy – Appendix A

Internet Safety Program Summary & Curriculum– Appendix B

Email Usage Policy – Appendix C

Social Networking Policy – Appendix D

Student Tablet Guidelines – Appendix E

BYOD Guidelines – Appendix F

# **APPENDIX**

## **A**

<b>Title</b>	<b>ACCEPTABLE COMPUTER SYSTEM USE</b>
<b>Number</b>	<b>GAB/IIBE A</b>
<b>Legal</b>	18 U.S.C. Sections 1460, 2256, 47 U.S.C. Section 254, Code of Virginia, 1950, as amended, Sections 18.2-372, 18.2-374.1:1, 18.2-390, 22.1-70.2 and 22.1-78.
<b>Adopted</b>	February 8, 2011

The School Board provides a computer system, including the internet, to promote educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes hardware, software, data, communication lines and devices, terminals, printers, CD-ROM devices, tape drives, servers, mainframe and personal computers, the internet and other internal or external networks.

All use of the Division's computer system must be (1) in support of education and/or research, or (2) for legitimate school business. Use of the computer system is a privilege, not a right. Any communication or material used on the computer system, including electronic mail or other files deleted from a user's account, may be monitored or read by school officials.

The Division Superintendent shall establish administrative procedures, for the School Board's approval, containing the appropriate uses, ethics and protocol for the computer system.

The procedures shall include:

- a prohibition against use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing or downloading illegal material via the Internet;
- provisions, including the selection and operation of a technology protection measure for the division's computers having Internet access to filter or block Internet access through such computers, that seek to prevent access to
  - (a) child pornography as set out in Va. Code § 18.2-374.1:1 or as defined in 18 U.S.C. § 2256;
  - (b) obscenity as defined by Va. Code § 18.2-372 or 18 U.S.C. § 1460; and
  - (c) material that the school division deems to be harmful to juveniles as defined in Va. Code § 18.2-390, material that is harmful to minors as defined in 47 U.S.C. § 254(h)(7)(G), and material that is otherwise inappropriate for minors;
- provisions establishing that the technology protection measure is enforced during any use of the Division's computers by minors;
- provisions establishing that the online activities of minors will be monitored;
- provisions designed to educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response;
- provisions designed to prevent unauthorized online access by minors, including "hacking" and other unlawful activities by minors online; and
- provisions prohibiting the unauthorized disclosure, use, and dissemination of personal information regarding minors.

Use of the School Division's computer system shall be consistent with the educational or instructional mission or administrative function of the Division as well as the varied instructional needs, learning styles, abilities and developmental levels of students. The Division's computer system is not a public forum.

Each teacher, administrator, student and parent/guardian of each student shall sign the Acceptable Computer System Use Agreement, GAB-E1/IIBEA-E2, before using the Division's computer system. The failure of any student, teacher or administrator to follow the terms of the Agreement, this policy or accompanying regulation may result in loss of computer system privileges, disciplinary action, and/or appropriate legal action.

The School Board is not responsible for any information that may be lost, damaged or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the School Board will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

The school board will review, amend if necessary, and provide this policy every two years.

Cross Refs:     [GCPD Professional Staff Members: Contract Status and Discipline](#)  
                  [GDPD Support Staff Members: Contract Status and Discipline](#)  
                  [JFC Student Conduct](#)  
                  [JFC-R Standard of Student Conduct](#)





<b>Title</b>	<b>ACCEPTABLE COMPUTER SYSTEM USE - Regulations</b>
<b>Number</b>	<b>GAB-R/IIBEA-R</b>
<b>Status</b>	Active
<b>Legal</b>	18 U.S.C. §§ 1460, 2256, 47 U.S.C. § 254. Code of Virginia, 1950, as amended, §§ 18.2-372, 18.2-374.1:1, 18.2-390, 22.1-70.2, and 22.1-78 Guidelines and Resources for Internet Safety in Schools, Virginia Department of Education (Second Edition October 2007)
<b>Adopted</b>	September 8, 2009

All use of the Dinwiddie School Division's computer system shall be consistent with the School Board's goal of promoting educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes hardware, software, data, communication lines and devices, terminals, printers, CD-ROM devices, tape drives, servers, mainframe and personal computers, the internet and any other internal or external network.

#### **Computer System Use-Terms and Conditions:**

1. **Acceptable Use.** Access to the Division's computer system shall be (1) for the purposes of education or research and be consistent with the educational objectives of the Division or (2) for legitimate school business.
2. **Privilege.** The use of the Division's computer system is a privilege, not a right.
3. **Unacceptable Use.** Each user is responsible for his or her actions on the computer system. Prohibited conduct includes but is not limited to:
  - using the network for any illegal or unauthorized activity, including violation of copyright or contracts, or transmitting any material in violation of any federal, state, or local law.
  - sending, receiving, viewing or downloading illegal material via the computer system.
  - unauthorized downloading of software.
  - using the computer system for private financial or commercial purposes.
  - wastefully using resources, such as file space.
  - gaining unauthorized access to resources or entities.
  - posting material created by another without his or her consent.
  - submitting, posting, publishing, or displaying any obscene, profane, threatening, illegal, or other inappropriate material.
  - using the computer system while access privileges are suspended or revoked.
  - vandalizing the computer system, including destroying data by creating or spreading viruses or by other means.
  - intimidating, harassing, or coercing others.
  - threatening illegal or immoral acts.
4. **Network Etiquette.** Each user is expected to abide by generally accepted rules of etiquette, including the following:

- be polite.
- users shall not forge, intercept or interfere with electronic mail messages.
- use appropriate language. The use of obscene, lewd, profane, lascivious, threatening or disrespectful language is prohibited.
- users shall not post personal information other than directory information as defined in Policy JO Student Records about themselves or others.
- users shall respect the computer system's resource limits.
- users shall not post chain letters or download large files.
- users shall not use the computer system to disrupt others.
- users shall not modify or delete data owned by others.

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

**6. Security.** Computer system security is a high priority for the school division. If any user identifies a security problem, the user shall notify the building principal or system administrator immediately. All users shall keep their passwords confidential and shall follow computer virus protection procedures.

**7. Vandalism.** Intentional destruction of or interference with any part of the computer system through creating or downloading computer viruses or by any other means is prohibited.

**8. Charges.** The School Division assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including telephone or long-distance charges.

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

**10. Enforcement.** Software will be installed on the division's computers having Internet access to filter or block internet access through such computers to child pornography and obscenity. The online activities of users may also be monitored manually.

**Any violation of these regulations shall result in loss of computer system privileges and may also result in appropriate disciplinary action, as determined by School Board policy, or legal action.**

**Cross Ref.:** [GCPD](#) Professional Staff Members: Contract Status and Discipline  
[GDPD](#) Support Staff Members: Contract Status and Discipline  
[JFC](#) Student Conduct  
[JFC-R](#) Standards of Student Conduct

## **APPENDIX B**

### **Internet Safety Program Summary**

Based on feedback and results of our Internet Safety Program that we have conducted, we plan to modify portions of our program for students. Overall, we learned that students know the answers when asked about internet safety and usage; however, we continue to see that they do not put that into practice.

***Elementary*** - We plan to continue with our lessons we are doing; however, we have learned that we need to educate the parents more, especially about social networking. Many students are involved with social networking and many parents are unaware. More emphasis will be placed at back to school night in the fall.

***Secondary*** - We are seeing an increase in the number of behavior issues related to internet and social networking. Students know right from wrong when asked about the dangers of internet, but they certainly are not putting that into use. For a recent series of internet safety lessons at our middle school, we did presentations that were class specific. The ITRT took the class roster and spent no more than 1-2 minutes per child and did an internet search. While we were not surprised what we found, the students were! They gained a greater understanding for setting their security and what to share and not share on social networking sites. This presentation was so successful that we plan to do this for all of our secondary classes next year when we conduct our internet safety lessons. We also plan to focus more attention on parent education as well.

Dinwiddie County Public Schools  
Internet Safety  
Grades K-12, Staff, Parent, and Community

Internet Safety Scope and Sequence	
Grade K	<ol style="list-style-type: none"> <li>1. Is This Yours? – Children learn that computers, like other objects, are property and should be respected. <a href="http://www.cybersmartcurriculum.org/lesson_plans/k1_02.asp">http://www.cybersmartcurriculum.org/lesson_plans/k1_02.asp</a></li> <li>2. Clicky’s Web World – What to Do on the Web – This activity explains things that you can do on the World Wide Web. <a href="http://www.netsmartzkids.org/activities/clwebworld/clwhat2do.htm">http://www.netsmartzkids.org/activities/clwebworld/clwhat2do.htm</a>  Kidspiration Activity – What to Do on the Web – This is a Kidspiration template that students will sort through pictures that represent things that you can and cannot do on the Internet.  Clicky Coloring Sheet—<i>For students to complete when you leave.</i></li> <li>3. CyberSpace at School - Children explore the concept of cyberspace as a means of communicating with <i>real</i> people within their school. <a href="http://www.cybersmartcurriculum.org/lesson_plans/k1_07.asp">http://www.cybersmartcurriculum.org/lesson_plans/k1_07.asp</a></li> <li>4. NetSmartz – Clicky, the NetSmartz spokesrobot introduces children to the Webville Outlaws. This video discusses dangers that children may encounter on the Internet.  Welcome to Webville Coloring Sheet—For students to complete when you leave.</li> <li>5. Clicky’s Web World - Webville Outlaw – Discusses dangers that children could face online. <a href="http://www.netsmartzkids.org/activities/clwebworld/outlaws.htm">http://www.netsmartzkids.org/activities/clwebworld/outlaws.htm</a>  Clicky’s Challenge – Name That Outlaw – Students will recognize different Types of dangers online. <a href="http://www.netsmartzkids.org/activities/clwebworld/clchalng.htm">http://www.netsmartzkids.org/activities/clwebworld/clchalng.htm</a>  <b>Additional Activity:</b> Clicky’s Race to the Finish Game <a href="http://www.netsmartz.org/pdf/Clicky_Race_to_the_Finish.pdf">http://www.netsmartz.org/pdf/Clicky_Race_to_the_Finish.pdf</a></li> </ol>
Grade 1	<ol style="list-style-type: none"> <li>1. Is This Yours? – Children learn that computers, like other objects, are property and should be respected. <a href="http://www.cybersmartcurriculum.org/lesson_plans/k1_02.asp">http://www.cybersmartcurriculum.org/lesson_plans/k1_02.asp</a></li> <li>2. Clicky’s Web World – What to Do on the Web – explains things that you can do on the World Wide Web <a href="http://www.netsmartzkids.org/activities/clwebworld/clwhat2do.htm">http://www.netsmartzkids.org/activities/clwebworld/clwhat2do.htm</a>  Kidspiration Activity – What to Do on the Web - This is a Kidspiration template that students will sort through pictures that represent things that you can and cannot do on the Internet.</li> </ol>

	<p>Clicky Coloring Sheet—<i>For students to complete when you leave.</i></p> <ol style="list-style-type: none"> <li>NetSmartz – Clicky, the NetSmartz spokesrobot introduces children to the Webville Outlaws. These characters underscore the risk of giving out any personal information.</li> <li>Clicky’s Web World - Webville Outlaw – Discusses dangers that children could face online.  <a href="http://www.netsmartzkids.org/activities/clwebworld/outlaws.htm">http://www.netsmartzkids.org/activities/clwebworld/outlaws.htm</a></li> </ol> <p>Clicky’s Challenge – Name That Outlaw  <a href="http://www.netsmartzkids.org/activities/clwebworld/clchalng.htm">http://www.netsmartzkids.org/activities/clwebworld/clchalng.htm</a></p> <p><b>Additional Activity:</b> Clicky’s Race to the Finish Game  <a href="http://www.netsmartz.org/pdf/Clicky_Race_to_the_Finish.pdf">http://www.netsmartz.org/pdf/Clicky_Race_to_the_Finish.pdf</a></p> <ol style="list-style-type: none"> <li>Spread the News - Children learn what it means to communicate, recognize the computer as a communication invention, and plan their own way to communicate a message.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/k1_08.asp">http://www.cybersmartcurriculum.org/lesson_plans/k1_08.asp</a></li> <li>Find the Ad - Children learn that the purpose of advertisements is to encourage people to buy something; children also practice differentiating ads from content on Web sites.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/k1_03.asp">http://www.cybersmartcurriculum.org/lesson_plans/k1_03.asp</a></li> </ol>
Grade 2	<ol style="list-style-type: none"> <li>Faux Paws Video – Faux Paw the Techno Cat discusses the importance of Protecting personal information and avoiding inappropriate places on the Internet.   Surf Swell Island  <a href="http://disney.go.com/surfswell/index.html?name=ac_med6_surfSwell">http://disney.go.com/surfswell/index.html?name=ac_med6_surfSwell</a></li> <li>Whose Property Is This? - Students extend their understanding of "property" to include not only computer equipment but also the work of others, and then discuss rules for respecting such property.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/23_02.asp">http://www.cybersmartcurriculum.org/lesson_plans/23_02.asp</a></li> <li>My CyberSpace Neighborhood – Students explore the concept of cyberspace as a means of connecting people and explain how the ability for people to communicate can unite a neighborhood.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/23_12.asp">http://www.cybersmartcurriculum.org/lesson_plans/23_12.asp</a></li> <li>What’s Private - Children learn about the power of the Internet to facilitate collaboration among students worldwide. While co-writing a story online, students learn an important safety rule: Before sharing private information in cyberspace, they must get permission from a parent or teacher.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/23_01.asp">http://www.cybersmartcurriculum.org/lesson_plans/23_01.asp</a></li> <li>Go Places Safely – Lesson plan on how to navigate a website  <a href="http://www.cybersmartcurriculum.org/lesson_plans/k1_01.asp">http://www.cybersmartcurriculum.org/lesson_plans/k1_01.asp</a></li> <li>Things for Sale - Students learn that some Web sites are advertising environments intended to promote good feelings about products.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/23_04.asp">http://www.cybersmartcurriculum.org/lesson_plans/23_04.asp</a></li> </ol>

Grade 3	<ol style="list-style-type: none"> <li>1. Understand Your Acceptable Use Policy - Students will interpret and make inferences about their school's AUP. <a href="http://www.cybersmartcurriculum.org/lesson_plans/45_07.asp">http://www.cybersmartcurriculum.org/lesson_plans/45_07.asp</a></li> <li>2. Netti and Webster Cyber-siblings Video – NetSmarts Netti and Webster talk with children about online dangers.  Safe Surfing with Dongle <a href="http://www.kidsmart.org.uk/movies/Safe_Surfing.swf">http://www.kidsmart.org.uk/movies/Safe_Surfing.swf</a></li> <li>3. CyberSpace Country - Students contrast cyberspace with actual and fantasy places, learning that cyberspace is where <i>real</i> people connect using computers and <i>real</i> experiences take place. Then they visually express their understanding of the geography of cyberspace in the U.S. <a href="http://www.cybersmartcurriculum.org/lesson_plans/45_19.asp">http://www.cybersmartcurriculum.org/lesson_plans/45_19.asp</a></li> <li>4. Who's Your Friend on the Internet <a href="http://www.netsmartkids.org/activities/nsrules/whofriend.htm">http://www.netsmartkids.org/activities/nsrules/whofriend.htm</a></li> <li>5. Good Manners Everywhere - Students discuss good manners in the real world and learn some do's and don'ts when using E-mail in cyberspace. <a href="http://www.cybersmartcurriculum.org/lesson_plans/23_03.asp">http://www.cybersmartcurriculum.org/lesson_plans/23_03.asp</a></li> <li>6. Filling Out a Form - Students learn that many Web sites have enticing offers in exchange for information and discuss how to responsibly handle such offers. <a href="http://www.cybersmartcurriculum.org/lesson_plans/23_05.asp">http://www.cybersmartcurriculum.org/lesson_plans/23_05.asp</a></li> </ol>
Grade 4	<ol style="list-style-type: none"> <li>1. Understand Your Acceptable Use Policy – Students will interpret and make inferences about their school's AUP. <a href="http://www.cybersmartcurriculum.org/lesson_plans/45_07.asp">http://www.cybersmartcurriculum.org/lesson_plans/45_07.asp</a></li> <li>2. Internet Safety DVD – This movie presented by John Walsh and Julie Clark discuss hot tips to keep cool kids safer on the Internet.  Internet Safety – What if scenarios. <a href="http://www.sbac.edu/~media/5%20Rules%20for%20Internet%20Safety.pdf">http://www.sbac.edu/~media/5%20Rules%20for%20Internet%20Safety.pdf</a></li> <li>3. Do the Right Thing - Students learn that they should apply the same ethical principles in cyberspace that guide them in face-to-face situations <a href="http://www.cybersmartcurriculum.org/lesson_plans/45_09.asp">http://www.cybersmartcurriculum.org/lesson_plans/45_09.asp</a></li> <li>4. The First Adventures of the Three CyberPigs – Personal Information <a href="http://www.media-awareness.ca/english/special_initiatives/games/privacy_playground/flash/start.html">http://www.media-awareness.ca/english/special_initiatives/games/privacy_playground/flash/start.html</a></li> <li>5. The Second Adventure of the Three CyberPigs- Chat Rooms <a href="http://www.media-awareness.ca/english/special_initiatives/games/cybersense_nonsense/flash/start.html">http://www.media-awareness.ca/english/special_initiatives/games/cybersense_nonsense/flash/start.html</a></li> <li>6. What is a network? - Students model a network and learn that the Internet consists of many computer networks that are able to communicate with one</li> </ol>



	<p>another.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/45_20.asp">http://www.cybersmartcurriculum.org/lesson_plans/45_20.asp</a></p> <p>7. Using Categories with Keywords -Students learn that adding keywords in combination with a category search provides more specific results. They choose the subject of a biography by browsing through subject categories, narrowing their focus with selected keywords, and evaluating their search results.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/45_15.asp">http://www.cybersmartcurriculum.org/lesson_plans/45_15.asp</a></p>
Grade 5	<p>1. Understand Your Acceptable Use Policy - Students will interpret and make inferences about their school's AUP.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/45_07.asp">http://www.cybersmartcurriculum.org/lesson_plans/45_07.asp</a></p> <p>2. National Crime Prevention Activity ---- Who Am I?</p> <ul style="list-style-type: none"> <li>• Identify dangers on the Internet</li> <li>• To build critical-thinking and decision-making skills  <a href="http://www.ncpc.org/law/internet1.php">http://www.ncpc.org/law/internet1.php</a></li> </ul> <p>3. Internet Safety Online Quiz  <a href="http://www.safekids.com/quiz/index.html">http://www.safekids.com/quiz/index.html</a></p> <p>Private Information - By examining and identifying actual online requests for private information, students learn to apply the same safety rules in cyberspace as they use when encountering strangers in the face-to-face world.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/45_01.asp">http://www.cybersmartcurriculum.org/lesson_plans/45_01.asp</a></p> <p>4. Cyber Café</p> <ul style="list-style-type: none"> <li>• Interactive website to promote online safety</li> <li>• Identifies dangers associated with <ul style="list-style-type: none"> <li>➤ Email</li> <li>➤ Chat Rooms</li> <li>➤ Instant Messaging</li> <li>➤ Web Browsing</li> <li>➤ Text Messaging</li> </ul> <a href="http://www.gridclub.com/teachers/t_internet_safety.html">http://www.gridclub.com/teachers/t_internet_safety.html</a></li> </ul> <p>5. Whose is it Anyway? - Students learn that, although the Internet makes it very easy, copying others' work and presenting it as one's own is unethical. They also learn about circumstances in which it is permissible to copy others' work.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/45_08.asp">http://www.cybersmartcurriculum.org/lesson_plans/45_08.asp</a></p> <p>CyberTreehouse – Go to games and then the Q&amp;A Game  This activity contains 5 questions that cover piracy, copyright, and password privacy.  <a href="http://www.cybertreehouse.com/">http://www.cybertreehouse.com/</a></p> <p>6. Rating Websites - Students discuss and apply criteria for rating informational Web sites, compare their results, and infer that all Web sites are not equally good sources of research information.  <a href="http://www.cybersmartcurriculum.org/lesson_plans/45_16.asp">http://www.cybersmartcurriculum.org/lesson_plans/45_16.asp</a></p> <p>7. Safe Talking in Cyberspace - Students explore positive aspects of online chatting and messaging, consider a potentially uncomfortable scenario, and learn to apply</p>

	<p>safety rules that protect their private identity information  <a href="http://www.cybersmartcurriculum.org/lesson_plans/45_04.asp">http://www.cybersmartcurriculum.org/lesson_plans/45_04.asp</a></p>
Grades 6-8	<ul style="list-style-type: none"> <li><input type="checkbox"/> Internet Safety Guide information from DOE booklet, p. 7-9 and Appendix D</li> <li><input type="checkbox"/> <b>screennames/personal information/password security</b></li> <li><input type="checkbox"/> Study Island/Edline</li> <li><input type="checkbox"/> <b>"You won! Collect your prize here!"</b></li> <li><input type="checkbox"/> <b>copyright/music piracy</b></li> <li><input type="checkbox"/> PhotoStory or Audacity</li> <li><input type="checkbox"/> <b>appropriate web searching, web extensions</b></li> <li><input type="checkbox"/> Research</li> <li><input type="checkbox"/> <b>appropriate email</b> - English</li> <li><input type="checkbox"/> <b>Instant Messaging</b> - English</li> <li><input type="checkbox"/> <b>MySpace, etc.</b> -Civics (freedom of speech, privacy)</li> <li><input type="checkbox"/> 7 Things You Should Know About You Tube handout</li> <li><input type="checkbox"/> 7 Things You Should Know About Facebook handout</li> <li><input type="checkbox"/> 7 Things You Should Know About Social Bookmarking handout</li> <li><input type="checkbox"/> 7 Things You Should Know About Instant Messaging handout</li> <li><input type="checkbox"/> A Guide to MySpace &amp; MySpace Safety Tips handout</li> <li><input type="checkbox"/> Safeguarding Kids Online Activities</li> <li><input type="checkbox"/> Blogging Tips</li> </ul>
Grades 9 - 12	<ul style="list-style-type: none"> <li><input type="checkbox"/> Presentation during student handbook briefing (PPT &amp; brochure)</li> <li><input type="checkbox"/> Internet Safety Guide information from DOE booklet, p. 7-9 and Appendix D</li> <li><input type="checkbox"/> Presentation during library orientation (PPT – different than other PPT, posters)</li> <li><input type="checkbox"/> Guidance (Provide info sources, brochures)</li> <li><input type="checkbox"/> Cyber Week (See iSafe curriculum)</li> <li><input type="checkbox"/> Password/ScreenName security</li> <li><input type="checkbox"/> E-mail safety/security &amp; Computer security (offers, pop-ups, phishing, viruses, malware)</li> <li><input type="checkbox"/> Social Networking sites (Communicating w/ strangers, providing personal information, )</li> <li><input type="checkbox"/> Appropriate use of e-mail/e-mail etiquette</li> <li><input type="checkbox"/> Instant messaging/text messaging (providing personal information, privacy, safety)</li> <li><input type="checkbox"/> Copyright (music, plagiarism, sites that allow students to download school work, )</li> <li><input type="checkbox"/> Participating in forums (Message boards, chat rooms, )</li> <li><input type="checkbox"/> Cyber bullying</li> <li><input type="checkbox"/> 7 Things You Should Know About You Tube handout</li> <li><input type="checkbox"/> 7 Things You Should Know About Facebook handout</li> <li><input type="checkbox"/> 7 Things You Should Know About Social Bookmarking handout</li> <li><input type="checkbox"/> 7 Things You Should Know About Instant Messaging handout</li> <li><input type="checkbox"/> A Guide to MySpace &amp; MySpace Safety Tips handout</li> <li><input type="checkbox"/> Safeguarding Kids Online Activities</li> <li><input type="checkbox"/> Blogging Tips</li> </ul>
Staff	<ul style="list-style-type: none"> <li><input type="checkbox"/> Sign Acceptable Use Policy</li> <li><input type="checkbox"/> Internet Safety Guide information from DOE booklet, p. 13-15 and Appendix D</li> <li><input type="checkbox"/> Administrators - Internet Safety Guide information from DOE booklet, p. 16-17 and Appendix D</li> </ul>

	<input type="checkbox"/> Beginning of school year (PPT) <input type="checkbox"/> School web site/Edline (Upload PPT, Link brochures) <input type="checkbox"/> Cyber Week (See iSafe curriculum) <input type="checkbox"/> Cyberbullying Paper (for administrators) <input type="checkbox"/> Faculty Insider – Instant Messenger handout <input type="checkbox"/> 7 Things You Should Know About You Tube handout <input type="checkbox"/> 7 Things You Should Know About Facebook handout <input type="checkbox"/> 7 Things You Should Know About Social Bookmarking handout <input type="checkbox"/> 7 Things You Should Know About Instant Messaging handout <input type="checkbox"/> A Guide to MySpace & MySpace Safety Tips handout <input type="checkbox"/> Safeguarding Kids Online Activities <input type="checkbox"/> Blogging Tips
Parents & Community	<input type="checkbox"/> Back to school night & parent night (brochure, kiosk) <input type="checkbox"/> Internet Safety Guide information from DOE booklet, p. 10-12 and Appendix D <input type="checkbox"/> Monitor (monthly or weekly articles) September is Internet Safety month <input type="checkbox"/> School web site/Edline (Upload PPT, Link brochures) <input type="checkbox"/> School newsletter (articles) <input type="checkbox"/> Distribute “Keeping Kids Safer in the Internet” brochure (September) <input type="checkbox"/> Distribute “Your Kids can fill in the blanks. Can you?” brochure (September) <input type="checkbox"/> Parents Guide to Protect Children on the Internet handout <input type="checkbox"/> 7 Things You Should Know About You Tube handout <input type="checkbox"/> 7 Things You Should Know About Facebook handout <input type="checkbox"/> 7 Things You Should Know About Social Bookmarking handout <input type="checkbox"/> 7 Things You Should Know About Instant Messaging handout <input type="checkbox"/> A Guide to MySpace & MySpace Safety Tips handout <input type="checkbox"/> Safeguarding Kids Online Activities <input type="checkbox"/> Blogging Tips

# **APPENDIX**

## **C**

# **Dinwiddie County Public Schools**

## **E-mail Usage Policy**

### **Introduction**

**This policy sets out the general rules and guidelines for use of electronic mail (e-mail) in the Dinwiddie County Public Schools (DCPS), including electronic notice-boards hosted therein. E-mail and other electronic information systems will reduce the need for paper-based communication. DCPS makes an e-mail system available and encourages the appropriate use of e-mail as an alternative to paper based communication.**

**The DCPS e-mail system is coordinated and managed by the Department of Technology. No other e-mail system (server or client) is recognized or supported by DCPS.**

### **Use of E-mail**

**The e-mail system is DCPS property and DCPS reserves the right to monitor and to access any e-mail messages. The use of e-mail for personal purposes is permitted for convenience. All users are responsible for ensuring that their e-mail usage is within regulations and is ethical and lawful. The sending of text or images that contain material of an offensive, indecent or obscene nature is prohibited.**

**Provided the appropriate security guidelines are followed, e-mails sent from one user to another on the same e-mail system are relatively secure - any other e-mails should at all times be regarded as having the same status as a postcard.**

**Users of e-mail should be aware of formal requirements and good practice in the use of e-mail as set out in the sections below.**

**E-mail may be used for any legal activity in furtherance of the aims or policies of DCPS, subject to the conditions listed below. The following specific uses are excluded:**

- Any use that violates DCPS policies, standards or administrative notices;**
- The use of another individual's e-mail account using that individual's identity (i.e. the individual's username/password details);**
- Impersonation or misrepresentation of another individual;**
- Alterations of source or destination address information;**
- The use of e-mail that could result in the inadvertent commitment of DCPS to a contract or agreement if it appears to the other party that he/she has authority to do so;**

- The use of e-mail for personal reasons to promote or denigrate companies or organizations, or defame other employees.

## Misuse of E-mail

Penalties for misuse of e-mail will depend on the seriousness of the offence, and be in accordance with current DCPS Procedures.

## Code of Practice for E-mail Users

Users should make every effort to adhere to the following guidelines for appropriate use:

- Check your e-mails regularly;
- Be polite. Messages sent by e-mail can often seem abrupt, even when this is not the intention. Use professional courtesy and discretion. The use of all upper-case text in either the subject or the body of an e-mail should also be avoided as this is deemed to be the e-mail equivalent of shouting;
- Do not reply with history of message if it is not necessary, especially if it incorporates a large attachment.
- Do not use "Reply to All" and distribution lists unless the message is relevant to all the specified recipients in order to keep the number of your messages to a minimum and reduce the risk of sending messages to the wrong people;
- Set the Auto Responder (Out-of-Office) to deal with your e-mail if you are away;
- Messages should be clearly addressed to those from whom an action or response is expected, "cc" or "bcc" should be used for other recipients of the message;
- Respect privacy and consider this aspect before forwarding messages;
- Delete unwanted or unnecessary e-mail. It is the user's responsibility to manage their own e-mail folders and keep within the quota limits set. The Technology Department can give advice and assistance if required;
- Unsolicited e-mail, especially with an attachment, may contain a virus. If in doubt, delete the e-mail or contact the Technology Department before opening if possible;
- Do not attempt to carry out confidential or sensitive tasks exclusively by e-mail;
- Enter a meaningful 'Subject' field to help the reader anticipate the content correctly;
- Do not use all or part of someone else's message without acknowledgement. Do not edit someone else's message without making clear the changes that you have made and do not distribute other people's messages without permission;
- Avoid subscribing to unnecessary mailing lists. Unsubscribe from mailing lists when they are no longer required;
- E-mail group lists provided by the Technology Department should be used for matters of DCPS or individual school business. Use of multiple e-mail group lists should be avoided unless absolutely necessary. Prior permission from the Technology Department is required to send a message to all users;
- Do not forward e-mail "chain letters". These are e-mails which either ask you to forward them on to all your friends (or to everyone you know) or which state that something bad will happen if you do not forward them on. E-mails of this type, including those warning about something (e.g. computer viruses), are almost certainly hoaxes;
- If you are unsure about any e-mail that you've received, contact the Technology Department for assistance.

## Cautionary Notes

The nature of e-mail is such that total confidentiality cannot be guaranteed and users should be aware of the following points about the use of e-mail:

- Copies of e-mail may exist on a back-up copy or a remote system even after the author or recipient has deleted the message;
- E-mail may be forwarded by any recipient without the author's consent, although it may not have been the author's intention. A forwarded message may be a modified version of the original;
- It is possible for the author or sender of an e-mail to disguise or alter their identity;
- Organizations outside DCPS may have different policies on e-mail. Some consider it the property of the organization, subject to examination, copying or forwarding. Be aware of this possibility when sending e-mail;
- A reply to a personal message sent via a 'list server' or electronic bulletin board may be inadvertently distributed to all subscribers to the list;
- Usernames and passwords should not be disclosed to others. This could result in security breaches and other people using your e-mail account to send unauthorized messages. Suspected security breaches should be reported to the Technology Department at once;
- Once a message is sent, there is no way to recall it. Check carefully that messages are addressed to the correct recipient(s) before sending.

## Auditing

The Technology Department does not routinely monitor or access e-mail. All e-mails, however, arriving at Dinwiddie County Public Schools are automatically scanned for viruses and for "spam" content, i.e. whether they match unsolicited, nuisance, e-mails previously sent to the School DCPS - any such e-mails are blocked. Filtering/virus-scanning can never be 100% effective so any unsolicited e-mails/attachments should always be treated with caution. Similarly, an e-mail may be incorrectly marked as infected or "spam" and therefore some e-mails could be blocked unnecessarily. The Technology Department reserves the right of access to users' e-mail and audit logs on both the client workstation as well as the servers for legitimate purposes, such as investigation of complaints of misuse. Content and audit logs for both sent and received e-mail may be inspected (including personal e-mail) at any time without notice. Authorization must always be given by the Director of the Technology Department (or designee) for access to staff e-mail.

The Technology Department will endeavor to maintain privacy of e-mail. There may be special cases, however, when it is essential that e-mail messages are accessed due to, for example, illness of the owner of a mailbox. In these instances, on the request of the appropriate Administrative personnel and on the authorization of the Director of the Technology Department (or designee), the Technology Department may locate and make available e-mail messages for access by a member of staff. The owner of the mailbox will be notified in due course.

Certain authorized members of the Technology Department may necessarily have access to the contents of e-mail messages in the course of system administration. Any knowledge thus obtained will not be communicated to others, unless required for system administration.

The Technology Department reserves the right to take special actions in administering e-mail if this is essential to preserve the integrity or functionality of the systems. This may include the deletion of e-mail.

## Retention

DCPS has an automatic centralized system to archive e-mails. This enables DCPS to track down previous e-mails in respect of correspondence that would be significant in an internal or external matter (e.g. correspondence of a contractual nature). It will also be used to provide access to information, when required to do so, in response to a request for information pursuant to the Virginia Freedom of Information Act.

The e-mails are stored as part of an archiving system. Generally, e-mails will be archived for a period of no less than two calendar years.

## Deletion and Archiving

E-mail messages are archived along with other files in accordance with existing Technology Department operational procedures so messages deleted by users might still be held on archives. Archiving of e-mail messages, however, is not intended to act as a backup to user mailboxes and recovery will be limited to division critical messages. Users should make an effort to maintain their own essential messages.

## Security – Opening and Closing of Accounts

Computer and e-mail accounts for staff are set up by the Technology Department. Associated passwords are issued directly to the end user or via faculty staff.

Before leaving employment at Dinwiddie County Public Schools, staff should unsubscribe from any e-mail lists that they may have subscribed to and delete any personal e-mails in their account. If there are any work-related e-mails that need to be transferred to another user then these e-mails should be forwarded as appropriate – contact the Technology Department if assistance is required.

At the discretion of the DCPS Administration, following the departure of a member of staff from DCPS, that user's e-mail account will be disabled for a period of 2 weeks after which time the



account will be deleted. DCPS Administration may request access to the closed mailbox be given to another member of staff for this duration.

## Disclaimer

All e-mail messages sent from DCPS will include an e-mail disclaimer, as follows:

**“This transmission is confidential and may be legally privileged. If you are not the intended recipient, please notify the sender by return e-mail and delete the message from your system. Dinwiddie County Public Schools reserves the right to monitor e-mail communication through its network. No contract may be concluded on behalf of Dinwiddie County Public Schools by e-mail. If the content of this e-mail does not relate to the business of Dinwiddie County Public Schools, then we do not endorse it and will accept no liability.”**

## Review

**It is the responsibility of the Technology Department to review regularly the content of the Electronic Mail Usage Policy for relevancy.**

■  
■

**Statement of Agreement**

**By my signature below, I attest that I have read and will comply with the E-Mail Usage policy employed by Dinwiddie County Public Schools.**

**Printed Name:** \_\_\_\_\_

**Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

**School/Department:** \_\_\_\_\_

**DINWIDDIE COUNTY PUBLIC SCHOOLS**

# **APPENDIX**

## **D**

**Title   ACCEPTABLE COMPUTER SYSTEM USE (Use of Social Networking Sites by DCPS Employees - effective November 1, 2012))**

Number   IIBEA/GAB

Status   Active

Legal

18 U.S.C. Sections 1460, 2256, 47 U.S.C. Section 254, Code of Virginia, 1950, as amended, Sections 18.2-372, 18.2-374.1:1, 18.2-390, 22.1-70.2 and 22.1-78; Code of Virginia, 1950 as amended, 22.1-70.2, 18.2-372 and 18.2-374.1:1, 18.2-390; Children's Internet Protection Act (Federal Communications Commission Regulations);

Guidelines for the Prevention of Sexual Conduct and Abuse in Virginia Public Schools, Virginia Department of Education, March 24, 2011

Adopted   October 9, 2012

Last Revised   February 8, 2011

The School Board provides a computer system, including the internet, to promote educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes hardware, software, data, communication lines and devices, terminals, printers, CD-ROM devices, tape drives, servers, mainframe and personal computers, the internet and other internal or external networks.

All use of the Division's computer system must be (1) in support of education and/or research, or (2) for legitimate school business. Use of the computer system is a privilege, not a right. Any communication or material used on the computer system, including electronic mail or other files deleted from a user's account, may be monitored or read by school officials.

The Division Superintendent shall establish administrative procedures, for the School Board's approval, containing the appropriate uses, ethics and protocol for the computer system. The procedures shall include:

(1) a prohibition against use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing or downloading illegal material via the Internet;

(2) provisions, including the selection and operation of a technology protection measure for the division's computers having Internet access to filter or block Internet access through such computers, that seek to prevent access to

(3) provisions establishing that the technology protection measure is enforced during any use of the Division's computers by minors;

(4) provisions establishing that the online activities of minors will be monitored;

(5) provisions designed to educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response;

(6) provisions designed to prevent unauthorized online access by minors, including "hacking" and other unlawful activities by minors online; and

(7) provisions prohibiting the unauthorized disclosure, use, and dissemination of personal information regarding minors.

- a) child pornography as set out in Va. Code § 18.2-374.1:1 or as defined in 18 U.S.C. § 2256;
- b) obscenity as defined by Va. Code § 18.2-372 or 18 U.S.C. § 1460; and
- c) material that the school division deems to be harmful to juveniles as defined in Va. Code § 18.2-390, material that is harmful to minors as defined in 47 U.S.C. § 254(h)(7)(G), and material that is otherwise inappropriate for minors;

Use of the School Division's computer system shall be consistent with the educational or instructional mission or administrative function of the Division as well as the varied instructional needs, learning styles, abilities and developmental levels of students. The Division's computer system is not a public forum.

## **USE OF SOCIAL NETWORKING SITES BY DCPS EMPLOYEES**

**Effective, November 1, 2012**

### **A. Generally**

Dinwiddie County Public Schools (DCPS) recognizes the value of student, teacher, parent and community interaction on social networking sites that are designed for specific educational purposes and directly ties to DCPS curriculum and instruction. Collaboration, resource and information sharing, online tutoring, etc. can all be facilitated by the judicious use of educational internet/Web 2.0 networking tools and web pages, including, but not limited to, Facebook, Edmodo, Twitter, blogs, wikis, and other Web 2.0 networking tools.

A certified or licensed employee may communicate through electronic media with current DCPS students for educational purposes. All online communication via the DCPS network or in which an individual holds him/herself out as a DCPS employee must be consistent with DCPS policies and regulations.

### **B. Establishment of Social Networking Sites for Educational Purposes**

An employee may establish one or more social networking sites to be used for educational purposes and communication. Any such site shall have a clear statement of purpose and outcomes for the use of the networking tool, and a code of conduct for all site participants. The employee establishing the site shall: apply appropriate security settings, allow only approved participants access, be responsible for the site's content, diligently monitor the site for inappropriate content, and post only information related to the site's purpose that is appropriate for viewing by students, parents, and the community at large. Employees are expected to read and understand all terms of service and privacy policies associated with the social networking sites they intend to use.

### **C. Employee Use of Personal Social Networking Sites**

Employees shall make student internet safety, including the protection of students' personal information, a priority. DCPS therefore does not recommend that any employee establish an online social networking relationship with a currently enrolled DCPS student on his or her personal social networking site(s). For the protection and safety of both employee and students, employees should consider limiting internet contact and communication with such students to available school division-approved, work related social networking resources made available through the DCPS network.

In all use of personal social networking sites, employees should:

- Maintain appropriate professional boundaries as a classroom teacher, administrator, or supervisor;
- Practice online reputation management by considering the personal, professional and social impact of what you post;
- Establish appropriate privacy settings to limit access to personal information contained on your social networking site;
- Establish social networking relationships with caution and consider "un-friending" those who post inappropriate content that may be viewed on your social networking site;
- Refrain from inappropriate electronic communications with students;
- Recognize that students may not exercise good judgment and may use social media inappropriately;
- Avoid the appearance of impropriety;
- Refrain from posting negative information about students, parents, guardians, fellow employees or the school division;
- Refrain from uploading inappropriate content; exercise caution when posting links to Internet or social networking sites and consider ad-free sites for hosting videos to eliminate inadvertent access to inappropriate advertisements and content.

### **D. Consequences of Inappropriate Use of Social Networking**

All employees are expected to know and are responsible for observing federal and state laws as well as the School Board's policies and regulations pertinent to their work activities. This policy will be used in conjunction with the DCPS Acceptable Use Policy (GAB/IIBEA). Accordingly, employee use of social networking found to be in violation of one or more DCPS policies, regulations or procedures and/or in violation of any applicable state or federal law may result in disciplinary action, up to and including termination.

Each teacher, administrator, student and parent/guardian of each student shall sign the Acceptable Computer System Use Agreement, GAB-E1/IIBEA-E2, before using the Division's computer system. The failure of any student, teacher or administrator to follow the terms of the Agreement, this policy or accompanying regulation may result in loss of computer system privileges, disciplinary action, and/or appropriate legal action.

The School Board is not responsible for any information that may be lost, damaged or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the School Board will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

The school board will review, amend if necessary, and approve this policy every two years.

Cross Refs.: GCPD Professional Staff Members: Contract Status and Discipline  
GDPD Support Staff Members: Contract Status and Discipline

JFC - student Conduct

JFC-R Standards of Student Conduct

© 5/10 VSBA

DINWIDDIE COUNTY PUBLIC SCHOOLS

BoardDocs is intended for the use of subscribers and licensed customers.  
All users are required to read and follow the [acceptable use policy](#).  
[BoardDocs](#)® by Emerald Data Solutions, © 2002-2015.

**Title   ACCEPTABLE COMPUTER SYSTEM USE (Use of Social Networking Sites by DCPS Employees - Effective November 1, 2012)**

Number   GAB/IIBEA

Status   Active

Legal

18 U.S.C. Sections 1460, 2256, 47 U.S.C. Section 254, Code of Virginia, 1950, as amended, Sections 18.2-372, 18.2-374.1:1, 18.2-390, 22.1-70.2 and 22.1-78; Code of Virginia, 1950 as amended, 22.1-70.2, 18.2-372, and 18.2-374.1:1, 18.2-390; Children's Internet Protection Act (Federal Communications Commission Regulations); Guidelines for the Prevention of Sexual Conduct and Abuse in Virginia Public Schools, Virginia Department of Education, March 24, 2011

Adopted   July 9, 2013

Last Revised   October 9, 2012

The School Board provides a computer system, including the internet, to promote educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes, but is not limited to, hardware, software, data, communication lines and devices, terminals, printers, CD-ROM devices, tape or flash drives, servers, mainframe and personal computers, tablets, cellular phones, smart telephones, the internet and other internal or external networks.

All use of the Division's computer system must be (1) in support of education and/or research, or (2) for legitimate school business. Use of the computer system is a privilege, not a right. Any communication or material generated using the computer system, including electronic mail, instant or text messages, tweets, or other files deleted from a user's account, may be monitored, read, and/or archived by school officials.

The Division Superintendent shall establish administrative procedures, for the School Board's approval, containing the appropriate uses, ethics and protocol for the computer system.

The procedures shall include:

- (1) a prohibition against use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing or downloading illegal material via the Internet;
- (2) provisions, including the selection and operation of a technology protection measure for the division's computers having Internet access to filter or block Internet access through such computers, that seek to prevent access to
  - (a) child pornography as set out in Va. Code § 18.2-374.1:1 or as defined in 18 U.S.C. § 2256;
  - (b) obscenity as defined by Va. Code § 18.2-372 or 18 U.S.C. § 1460; and
  - (c) material that the school division deems to be harmful to juveniles as defined in Va. Code § 18.2-390, material that is harmful to minors as defined in 47 U.S.C. § 254(h)(7)(G), and material that is otherwise inappropriate for minors;
- (3) provisions establishing that the technology protection measure is enforced during any use of the Division's computers;
- (4) provisions establishing that all usage of the computer system may be monitored;
- (5) provisions designed to educate students and employees about appropriate online behavior, including interacting with students and other individuals on social networking websites and in chat rooms and cyberbullying awareness and response;
- (6) provisions designed to prevent unauthorized online access by minors, including "hacking" and other unlawful online activities by minors online; and
- (7) provisions prohibiting the unauthorized disclosure, use, and dissemination of photographs and/or personal information of or regarding minors.



- a) child pornography as set out in Va. Code § 18.2-374.1:1 or as defined in 18 U.S.C. § 2256;
- b) obscenity as defined by Va. Code § 18.2-372 or 18 U.S.C. § 1460; and
- c) material that the school division deems to be harmful to juveniles as defined in Va. Code § 18.2-390, material that is harmful to minors as defined in 47 U.S.C. § 254(h)(7)(G), and material that is otherwise inappropriate for minors;

Use of the School Division's computer system shall be consistent with the educational or instructional mission or administrative function of the Division as well as the varied instructional needs, learning styles, abilities and developmental levels of students. The Division's computer system is not a public forum.

## **USE OF SOCIAL NETWORKING SITES BY DCPS EMPLOYEES**

**Effective November 1, 2012**

### **A. Generally**

Dinwiddie County Public Schools (DCPS) recognizes the value of student, teacher, parent and community interaction on social networking sites that are designed for specific educational purposes and directly ties to DCPS curriculum and instruction. Collaboration, resource and information sharing, online tutoring, etc. can all be facilitated by the judicious use of educational internet/Web 2.0 networking tools and web pages, including, but not limited to, Facebook, Edmodo, Twitter, blogs, wikis, and other Web 2.0 networking tools.

A certified or licensed employee may communicate through electronic media with current DCPS students for educational purposes. All online communication via the DCPS network or in which an individual holds him/herself out as a DCPS employee must be consistent with DCPS policies and regulations.

### **B. Establishment of Social Networking Sites for Educational Purposes**

An employee may establish one or more social networking sites to be used for educational purposes and communication. Any such site shall have a clear statement of purpose and outcomes for the use of the networking tool, and a code of conduct for all site participants. The employee establishing the site shall: apply appropriate security settings, allow only approved participants access, be responsible for the site's content, diligently monitor the site for inappropriate content, and post only information related to the site's purpose that is appropriate for viewing by students, parents, and the community at large. Employees are expected to read and understand all terms of service and privacy policies associated with the social networking sites they intend to use.

### **C. Employee Use of Personal Social Networking Sites**

Employees shall make student internet safety, including the protection of students' personal information, a priority. DCPS therefore does not recommend that any employee establish an online social networking relationship with a currently enrolled DCPS student on his or her personal social networking site(s). For the protection and safety of both employee and students, employees should consider limiting internet contact and communication with such students to available school division-approved, work related social networking resources made available through the DCPS network.

In all use of personal social networking sites, employees should:

- Maintain appropriate professional boundaries as a classroom teacher, administrator, or supervisor;
- Practice online reputation management by considering the personal, professional and social impact of what you post;
- Establish appropriate privacy settings to limit access to personal information contained on your social networking site;
- Establish social networking relationships with caution and consider "un-friending" those who post inappropriate content that may be viewed on your social networking site;
- Refrain from inappropriate electronic communications with students;
- Recognize that students may not exercise good judgment and may use social media inappropriately;
- Avoid the appearance of impropriety;
- Refrain from posting negative information about students, parents, guardians, fellow employees or the school division;

- Refrain from uploading inappropriate content; exercise caution when posting links to Internet or social networking sites and consider ad-free sites for hosting videos to eliminate inadvertent access to inappropriate advertisements and content.

#### **D. Consequences of Inappropriate Use of Social Networking**

All employees are expected to know and are responsible for observing federal and state laws as well as the School Board's policies and regulations pertinent to their work activities. This policy will be used in conjunction with the DCPS Acceptable Use Policy (GAB/IIBEA). Accordingly, employee use of social networking found to be in violation of one or more DCPS policies, regulations or procedures and/or in violation of any applicable state or federal law may result in disciplinary action, up to and including termination.

Each teacher, administrator, student and parent/guardian of each student shall sign the Acceptable Computer System Use Agreement, GAB-E1/IIBEA-E2, before using the Division's computer system. The failure of any student, teacher or administrator to follow the terms of the Agreement, this policy or accompanying regulation may result in loss of computer system privileges, disciplinary action, and/or appropriate legal action.

The School Board is not responsible for any information that may be lost, damaged or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the School Board will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

The school board will review, amend if necessary, and provide this policy every two years.

Cross Refs: [GCPD Professional Staff Members: Contract Status and Discipline](#)  
[GDPD Support Staff Members: Contract Status and Discipline](#)  
[JFC Student Conduct](#)  
[JFC-R Standard of Student Conduct](#)

Title **ACCESS TO EMPLOYEE SOCIAL MEDIA ACCOUNTS**

Number **GAD**

Status **Active**

Legal

Code of Virginia, 1950, as amended, § 40.1-28.7:5

Adopted **August 11, 2015**

The Dinwiddie School Board does not require current or prospective employees to disclose the username or password to the employee's personal social media accounts or to add an employee, supervisor or administrator to the list of contacts associated with the employee's personal social media account.

If the School Board or a School Board employee inadvertently receives an employee's username and password to, or other login information associated with, the employee's personal social media account through the use of an electronic device provided to the employee by the School Board or a program that monitors the School Board's network, the Board will not be liable for having the information but will not use the information to gain access to the employee's social media account.

This policy does not prohibit the School Board and its agents from viewing information about a current or prospective employee that is publicly available.

This policy does not prohibit the School Board from requesting an employee to disclose the employee's username and password for the purpose of accessing a personal social media account if the employee's social media account activity is reasonably believed to be relevant to a formal investigation or related proceeding by the Board of allegations of an employee's violation of federal, state or local laws or regulations or of the Board's written policies. If the Board exercises its rights under this paragraph, the employee's username and password will only be used for the purpose of the formal investigation or a related proceeding.

Cross Ref.: GAB/IIBEA      Acceptable Computer System Use

# **APPENDIX**

## **E**

# **Dinwiddie County Public Schools Student Tablet Guidelines**



**2015-2016**

## TABLE OF CONTENTS

1. OVERVIEW
2. RECEIVING YOUR TABLET
3. TAKING CARE OF YOUR TABLET
  - 3.1 General Precautions
  - 3.2 Screen Care
4. USING YOUR TABLET AT SCHOOL
  - 4.1 Tablets Undergoing Repair
  - 4.2 Charging Your Tablet Battery
  - 4.3 Screensavers
  - 4.4 Sound
  - 4.5 Printing
  - 4.6 Tablet left at home
  - 4.7 E-mails
  - 4.8 Camera
5. MANAGING YOUR FILES & SAVING YOUR WORK
  - 5.1 Saving to My Documents
  - 5.2 Saving Data to Removable Storage Devices
6. SOFTWARE ON TABLETS
  - 6.1 Originally Installed Software
  - 6.2 Virus Protection
  - 6.3 Additional Software
  - 6.4 Inspection
  - 6.5 Software Upgrades
7. ACCEPTABLE USE
  - 7.1 General Guidelines
  - 7.2 Privacy and Safety
  - 7.3 Legal Propriety
  - 7.4 E-mail
  - 7.5 Consequences
8. PROTECTING & STORING YOUR TABLET
  - 8.1 Tablet Identification
  - 8.2 Tablets Left in Unsupervised Areas
9. REPAIRING OR REPLACING YOUR TABLET
  - 9.1 Accidental Damage Protection
  - 9.2 Student Carelessness
  - 9.3 Optional Insurance Protection
  - 9.4 Claims
  - 9.5 Lost or Stolen Tablets
  - 9.6 Loaners
10. TABLET TECHNICAL SUPPORT
11. TABLET COLLECTION

STUDENT TECHNOLOGY USE AGREEMENT

TABLET USE AGREEMENT

## 1. OVERVIEW

Students in grades 9<sup>th</sup> -11<sup>th</sup> at Dinwiddie High School will be issued tablet computers for use as part of their educational curriculum. Dinwiddie County Public Schools (DCPS) believes that these tablet computers will help improve our students overall growth and help develop skills that are necessary in our 21<sup>st</sup> Century. These 21<sup>st</sup> Century skills include:

- Critical and creative thinking
- Problem solving skills
- Information and computer skills
- Interpersonal and self-direction skills
- Technology literacy
- Collaboration and communication in a global world
- Experience in an online learning community

The Dinwiddie County Public School System believes that the benefits to students from access to the Internet, in the form of informational resources and opportunities for communication and collaboration, exceed the disadvantages. Families need to be aware that Dinwiddie County Public Schools has advanced software for Internet content filtering and has procedures in place to protect our students from harmful materials. Filters may not block all offensive materials and/or students may find ways to access inappropriate materials.

The guidelines, procedures, and information within this manual apply to all tablet devices and related accessories (power cords, covers, etc.) used at Dinwiddie High School. Teachers may set additional requirements for use in their classrooms.

Once the tablet has been issued to a student, the tablet will stay with them for the remainder of the school year, or until they withdraw from school. Students will be responsible for bringing their tablet to school with them every day, taking it home at the end of the day, and charging it for use before the next day. It is important to note that these units stay with the students 24 hours a day, and are not left unsupervised at any time. At the end of the year the device will be returned to the school, and may be reimaged to include the curriculum the student will need for the following year. The next school year the student will be issued the same device.

Access to the tablet is a privilege that entails responsibility on the part of the user. **Student tablets are the exclusive property of Dinwiddie County Public Schools** and as such, they can be inspected for compliance of all policies and procedures. Students found out of compliance will be subject to disciplinary action and/or legal actions as warranted by Dinwiddie County Public Schools. **Dinwiddie County Public Schools does not accept responsibility for the loss of any student added software or data that is deleted due to a reformat or reimage.**



## 2. RECEIVING YOUR TABLET

Prior to each school year there will be a mandatory meeting for Parents and Students. Parents and students must attend this meeting prior to the student receiving his/her tablet for the first time. Beginning the 2014-15 school year all incoming freshmen and their parents will be required to attend this meeting along with any newly enrolled students prior to receiving their tablet. **Parents and Students must sign and return the *Student Tablet Use Agreement* before the tablet will be issued to the student.** Please review Chapter 9: “Repairing or Replacing Your Tablet” and be familiar with this policy. This clearly outlines the details of the coverage options available.

Tablets will be collected at the end of each school year for maintenance, cleaning, and software installations. Students will be re-issued their original tablet each school year.

## 3. TAKING CARE OF YOUR TABLET

Students are responsible for the general care of the tablet they have been issued by the school. Tablets that are broken or fail to work properly must be taken to the Tablet Help Desk.

### 3.1 General Precautions

1. No food or drink is allowed next to your tablet while it is in use.
2. Cords, cables, and removable storage devices must be inserted carefully into the tablet.
3. Tablets should be powered off when not in use to conserve battery life.
4. Tablets must remain free of any writing, drawing, stickers, or labels that are not the property of the Dinwiddie County Public Schools.
5. Tablets must never be left in an unlocked car or any unsecured or unsupervised area.
6. Tablets should never be stored in a vehicle in direct sunlight or view. Excessive heat from a closed vehicle can cause damage to the unit. Exposure to cold conditions can deplete the battery life.
7. Students are responsible for keeping their tablet battery charged for school each day.
8. Tablets should be within the protective case (the one provided by the school that you received on the tablet) at all times.

### 3.2 Screen Care

Tablet screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of the tablet when it is closed.
- Do not place anything near the tablet that could put pressure on the screen.
- Do not place anything in the carrying case that will press against the cover.
- Do not place anything on the keyboard before closing the lid (e.g. pens, pencils, or flash drives).
- Clean the screen with a soft, dry cloth or anti-static cloth.
- Be aware of jewelry around the tablet, as these items may scratch the screen.
- **Be careful when placing the tablet inside of backpacks.**
- **Do not clean the screen with Windex or any other glass cleaning product or use an alcohol based solvent. Use only a mildly damp rag if a dry, lint free cloth will not remove all of the dirt and grime.**

## **4. USING YOUR TABLET AT SCHOOL**

Given the school's availability of technology, students are expected to use these resources judiciously in accordance with the following guidelines. Tablets are intended for use at school each day. Students must be responsible to bring their tablet to all classes. The tablet has to be charged and with the student at all times. In the classroom the student must follow the teacher's direction on the use of the device for that particular class. Only visiting sites or use of programs instructed by the teacher are permitted.

### **4.1 Tablet Undergoing Repair**

Report any issues with your device to the Tablet Help Desk. Depending on the reason for repair, a loaner tablet may be issued to students. There will be Help Desk hours available before, during, and after school hours. These hours will be posted by the Help Desk.

### **4.2 Charging Your Tablet's Battery**

Tablets must be brought to school each day in a fully charged condition. Students need to charge their tablet each evening. Tablets should be charged with the correct AC adapter and USB cable. Tablets charge faster when the device is powered off.

### **4.3 Screensavers**

1. Inappropriate media may not be used as a screensaver.
2. Presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, and gang related symbols or pictures will result in disciplinary actions.
3. Passwords on screensavers are not to be used.
4. Hard drive passwords are forbidden. If used, students may be responsible for the cost of replacement hardware.

### **4.4 Sound**

1. Students must have personal earbuds/headphones to listen to audio. Students must provide his/her own earbuds/headphones.
2. Sound must be muted unless permission is granted by the teacher for instructional purposes.

### **4.5 Printing**

Tablet devices are not configured to print to a school printer. If you need to print a document you will need to save it in your Google Drive or to a personal flash drive and print it from a DCPS networked computer or from your house.

### **4.6 Tablet Left at Home**

Your tablet is considered an essential school material. If students fail to bring their device to school, they are responsible for completing course work as though they had their device with them. Students who forget to bring their device to school will be issued a warning; multiple instances of this will result in a disciplinary referral.

### **4.7 E-mail**

- 1 Students will be issued a school e-mail account. (Gmail)
- 2 The Gmail account assigned to each student will be used for school purposes. Use of other e-mail accounts is not supported.
- 3 Your Gmail e-mail account is subject to inspection by the school. Always use appropriate language.
- 4 Do not transmit language or material that is profane, obscene, abusive, or offensive to others.
- 5 Do not send mass e-mails, chain letters or spam.
- 6 Students should maintain high integrity with regard to e-mail content.

#### **4.8 Camera**

A student will only use the camera for educational purposes as instructed by the teacher. **Usage of devices is prohibited in but not limited to the following areas: bathrooms, locker rooms, and the cafeteria. Students are prohibited from taking pictures or videos of other people without their permission.** Pictures or videos may only be uploaded when instructed by a teacher. Under no circumstances will photos or videos of school employees or students be uploaded to social media sites.

### **5. MANAGING YOUR FILES & SAVING YOUR WORK**

#### **5.1 Saving to Google Drive**

Only files stored on *Google Drive* will be backed up and saved automatically.

#### **5.2 Saving Data to Removable Storage Devices**

Students should also back up all of their work at least once each week using removable file storage. Students are responsible for providing their own flash drives or external hard drives.

- Non-school related material should be saved to these removable storage devices.
- It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion.
- **Computer malfunctions are not an acceptable excuse for failing to submit work.**

### **6. SOFTWARE ON TABLETS**

#### **6.1 Originally Installed Software**

The software originally installed by Dinwiddie County Public Schools must remain on the tablet in usable condition and be easily accessible at all times.

The tablet is supplied with Microsoft Windows 8 and additional software. Licensed software provided with all new tablets includes:

- Anti-virus
- Google Chrome
- Microsoft Internet Explorer
- Microsoft Office 2010
- Assessment software
- Textbooks for select courses

DCPS may add software applications for use in a particular course. The licenses for this software require that the software be deleted from tablets at the completion of the course. Periodic checks of tablets will be made to ensure that students have deleted software that is no longer required in class and that the school has not exceeded its licenses.

#### **6.2 Virus Protection**

The tablet has anti-virus protection software. This software will scan the hard drive and external drives for known viruses on boot up. The virus software will be upgraded from the network. The school's storage server and e-mail server are also installed with virus protection software and hardware. Any attempt to disable virus protection will result in disciplinary action.

#### **6.3 Additional Software**

It is the responsibility of individual students to be aware of additional software programs and files loaded onto their tablet. Students are responsible for maintaining the integrity of software required for facilitating academic activities.

- DCPS installed software and firmware is considered top priority on the devices. If available storage becomes limited all personal software will be removed.
- Any additional software must be appropriate for the school environment and may not infringe on the productivity of the classroom setting.
- Students are responsible for ensuring that only software that is licensed to their tablet is loaded onto their computers.
- Violent games and computer images containing obscene or pornographic material are banned.

## **6.4 Software Upgrades**

Upgrade versions of licensed software are available on occasion. Students may be instructed to upgrade their software from the school's network.

## **6.5 Inspection**

Student tablets are the exclusive property of Dinwiddie County Public Schools and as such, can be inspected at any time for compliance of all policies and procedures. Students found out of compliance will be subject to disciplinary action as warranted by Dinwiddie County Public Schools. **Dinwiddie County Public Schools does not accept responsibility for the loss of any student added software or data that is deleted due to a re-format or re-image.**

# **7. ACCEPTABLE USE**

## **7.1 General Guidelines**

1. Students will have access to available forms of electronic media and communication which is in support of education and research and in support of the educational goals and objectives.
2. Students are responsible for their ethical and educational use of the technology resources.
3. Access to Dinwiddie County Public Schools technology resources is a privilege and not a right. Each employee, student and/or parent will be required to follow the Dinwiddie County Public Schools *Acceptable Use Policy*. The Acceptable Use Policy is listed in the *Code of Student Conduct* booklet.
4. Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to the following: confidential information, copyrighted material, threatening or obscene material, cyber-bullying, and computer viruses.
5. Any attempt to alter data, the configuration of a computer, or the files of another user, without the consent of the individual, school administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the Dinwiddie County Public Schools *Code of Student Conduct*.
6. Under no circumstances should hardware be modified.
7. Threatening or obscene material, cyber-bullying, engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terrorist, abusive, sexually explicit, threatening, stalking, demeaning or slanderous language will be subject to disciplinary action in accordance with the Dinwiddie County Public Schools *Code of Student Conduct*.
8. Use of electronic devices to cheat on assignments or assessments will result in disciplinary action.

## **7.2 Privacy and Safety**

- 1 All Internet traffic is subject to monitoring or review.
- 2 If you inadvertently access a web site that contains obscene, pornographic or otherwise offensive material, notify a teacher, technology administrator or school administrator immediately so that such sites can be blocked from further access. This is not merely a request; it is a responsibility.

- 3 Do not go into chat rooms or send chain letters without permission.
- 4 Do not open, use, or change computer files that do not belong to you.
- 5 Do not reveal your full name, phone number, home address, social security number, credit card numbers, password or passwords of other people.
- 6 Remember that storage is not guaranteed to be private or confidential.

### **7.3 Legal Propriety**

Comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If you are unsure, ask a teacher or parent.

- 1 Plagiarism is a violation of the Dinwiddie County Public Schools *Code of Student Conduct*. Give credit to all sources used, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.
- 2 Use or possession of hacking software is strictly prohibited and violators will be subject to Dinwiddie County Public Schools *Code of Student Conduct*. Violation of applicable state or federal laws will result in criminal prosecution or disciplinary action by DCPS.

### **7.4 E-mail**

- 1 Students will be issued a school e-mail account. (Gmail)
- 2 The Gmail account assigned to each student will be used for school purposes. Use of other e-mail accounts is not supported.
- 3 Your Gmail e-mail account is subject to inspection at any time by the school.
- 4 Always use appropriate language.
- 5 Do not transmit language or material that is profane, obscene, abusive, or offensive to others.
- 6 Do not send mass e-mails, chain letters or spam.
- 7 Students should maintain high integrity with regard to e-mail content.
- 8
- 9 Only the Gmail e-mail account assigned to each student is authorized for use on your student tablet. Use of Hotmail, Yahoo mail, etc. is prohibited; students using these accounts on a school issued tablet will be subject to disciplinary action.

### **7.5 Consequences**

The student in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use. Non-compliance with the DCPS *Student Tablet Guidelines* or DCPS *Acceptable Use Policy* will result in disciplinary action as outlined in the Dinwiddie County Public Schools *Code of Student Conduct*.

Electronic mail, network usage, and all stored files shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use. DCPS cooperates fully with local, state or federal officials in any investigation concerning or relating to violations of computer crime laws. Proper authorities will be given access to their content.

## **8. PROTECTING & STORING YOUR TABLET**

### **8.1 Tablet Identification**

Student tablets will be labeled in the manner specified by the school. Please do not remove any labels used to identify the tablet. Tablets can be identified in the following ways:

- Serial number
- MAC address
- Asset tag
- Student's name

## **8.2 Tablets Left Unsupervised**

*Under no circumstances should tablets be left unsupervised.*

Unsupervised areas include the school grounds and campus, the cafeteria, computer lab, commons area, locker rooms, library, unlocked classrooms, and hallways. Any computers left in these areas are in danger of being stolen.

Unsupervised tablets will be confiscated by staff and taken to administration. Disciplinary action may be taken for leaving your tablet in an unsupervised area.

The following table outlines consequences of Unsupervised Tablet Offenses.

<b>Unsupervised</b>	<b>Consequence</b>
1	Verbal warning
2	ISS and parent contact
3	Suspended tablet use until parent conference
4	Parent conference to determine future use of tablet

## **9. REPAIRING OR REPLACING YOUR TABLET**

Dinwiddie County Public Schools recognizes that with the implementation of the tablet initiative there is a need to protect the investment by both DCPS and the Student/Parent. The following outlines the various areas of protection: warranty, accidental damage protection and insurance.

### **9.1 Accidental Damage Protection**

The ASUS Accidental Damage Protection plan protects users from unintentional damages that result from electrical, mechanical, or other hardware failure for one year. This protection plan is limited to only one claim.

#### **What's Typically Covered?**

- Liquid spills on the keyboard making it non-functional
- Harsh tossing of a backpack to the floor resulting in a cracked screen
- Electrical surge and or fire damage that causes significant damage to the device

#### **What's Not Covered?**

- Cosmetic damage such as scratches, dents, and blemishes
- Incorrect / Inadequate installations or modifications
- Theft and or loss of the device and its components
- Damages caused by acts of God, nature, or war
- AC Adapters / USB Cables

Student tablet **abuse** is not considered accidental and the student/parent will be required to reimburse the district for the cost of the tablet's repairs.

Students that received tablets during the 2014-2015 school year are not eligible for the ASUS Accidental Damage Protection plan after June 30, 2015.

## **9.2 Student Carelessness**

Students must pay for damage to their tablet that is not attributable to normal wear and tear. The following fees will be assessed according to the list below:

Main Board	\$ 149
Touch Panel Glass 10.1"	\$ 60
Power Adapter	\$ 15
Power Cable	\$ 9
LCD Module	\$ 119
Battery	\$ 40
Keyboard	\$ 19
LCD Cover	\$ 19
Bottom Case	\$ 14
Touchpad	\$ 18
	Replacement Case \$ 20

## **9.3 Optional Insurance Protection**

Dinwiddie County High School has chosen Worth Ave. Group as the vendor of choice to insure school issued Asus Transformer Books distributed to students and faculty. **Insurance with Worth Ave. Group will protect the device against ACCIDENTAL DAMAGE, THEFT, FIRE, FLOOD, NATURAL DISASTERS, POWER SURGE and VANDALISM.** This insurance policy will provide full replacement cost coverage and will protect the item worldwide (both on and off school grounds). The policy is also transferable to a replacement unit. AC Adapters and USB cables are not covered by the Worth Ave. insurance.

### **Insurance Coverage**

- Unlimited Incidents
- Accidental Damage
- Fire/Flood Damage
- Drops/cracked screens/liquid spills
- Vandalism
- Liquid Submersion
- Natural Disasters
- Theft
- Power Surge Due To Lightning
- No cost deductible

Cost for 2015-2016 - \$34 for 1 year protection

If you plan to purchase this optional insurance plan, an application must be received and the \$34 fee paid PRIOR to receiving the tablet. The application period for the 2015-2016 ends on September 11, 2015. The only students eligible to add this optional plan after this date will be newly enrolled students.

## **9.4 Claims**

All warranty and insurance claims will be handled through the Tablet Help Desk. Students will complete a work order and submit it to the Tablet Help Desk. Please do not take your tablet to a third party vendor to have it repaired.

## **9.5 Lost or Stolen Tablets**

Lost or stolen tablets must be reported to the Technology Support Specialist-Mobile at the Tablet Help Desk immediately. **Lost tablets are not covered by any protection or warranty plan.** Lost tablets must be replaced at the full replacement value – approximately \$375. Stolen tablets are covered under the optional accidental protection plan. The parent/guardian must file a police report and provide a copy to the school so that an insurance claim can be made.

The following table outlines the action plan for stolen tablets.

	<b>Action Plan for Stolen Tablets</b>
1	Report problem to Teacher
2	Report problem to an Administrator
3	File a police report
4	Take police report to the Tablet Help Desk

## **9.6 Loaners**

A loaner tablet will be issued to students that must have their tablet sent in for repairs. All loaner tablets should be kept in the case provided with the loaner. Students are responsible for taking care of the loaner tablet and case. The loaner tablet must be turned in before the student will be able to receive their original tablet.

## **10. TABLET TECHNICAL SUPPORT**

The Technology Support Specialist-Mobile will coordinate the repair work for tablets. Services provided include the following:

- Hardware maintenance and repairs
- Password management
- User account support
- Operating system or software configuration support
- Application information
- Re-imaging hard drives
- Updates and software installations
- Coordination of warranty repairs

## **11. Tablet Collection**

If a student is expelled, suspended long-term or withdrawn, from Dinwiddie County Public Schools the tablet and all accessories must be turned into either the Guidance Department, an Administrator or the Tablet Help



Desk. Each student must sign/complete a tablet collection form. All fees for damages, missing items, etc. will be due upon collection.

**Dinwiddie High School**  
**Student Technology Use Agreement**  
**2015-2016**

1. I will take good care of my tablet and know that I will be issued the same tablet each year.
2. I will not leave the tablet unattended.
3. I will not loan out my tablet to other individuals.
4. I will know where my tablet is at all times.
5. I will charge my tablet's battery daily.
6. I will keep food and beverages away from my tablet since they may cause damage to the computer.
7. I will not disassemble any part of my tablet or attempt any repairs.
8. I will protect my tablet by only carrying it while in the approved case.
9. I will use my tablet in ways that are appropriate and educational.
10. I will not place decorations (such as stickers, markers, etc.) on the tablet.
11. I understand that my tablet is subject to inspection at any time without notice and remains the property of Dinwiddie County Public Schools.
12. I will follow the policies outlined in the *Student Tablet Guidelines* and *Acceptable Use Policy* while at school, as well as outside the school day.
13. I will file a police report in case of theft, vandalism, and other acts covered by insurance.
14. I will be responsible for all damage or loss caused by neglect or abuse.
15. I agree to pay for the replacement of my power cords, battery, case, keyboard and other parts in the event any of these items are lost or stolen.
16. I agree to return the tablet and accessories in good working condition.
17. I have read and understand the policies stated in the *Student Tablet Guidelines* (to include the *Acceptable Use Policy*).

Student Name (Please Print): \_\_\_\_\_

Student Signature: \_\_\_\_\_ Date: \_\_\_\_\_

I understand how the terms of this agreement and the policies listed in the Technology plan apply to my student and me. I also understand the district's insurance coverage of the tablet.

Parent/Guardian Name (Please Print): \_\_\_\_\_

Parent/Guardian Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**\* This form must be signed and returned to the school in order to receive tablet.**



# Dinwiddie County Public Schools

P.O. Box 7, 14016 Boydton Plank Road, Dinwiddie, Virginia 23041  
804-469-4198 or Fax: 804-469-4197

*A Place to Learn. A Place to Grow. A Place to Belong.*

## Dinwiddie High School Parent/Guardian Tablet Agreement 2015-2016

Please print all information.

Student Name:

Last Name	First name	Middle Name	Grade
-----------	------------	-------------	-------

Address:

Street	City	Zip Code
--------	------	----------

Telephone(s):

Home Phone	Work Phone	Other
------------	------------	-------

### Tablet Agreement

- ☐ Parent/Guardian agrees to read and accept all the terms of the Parent Tablet Orientation and Acceptable Technology Use Agreement, including fees for lost or damaged equipment.
- ☐ Parent/Guardian agrees that my child will participate in the DHS tablet program.
- ☐ Parent/Guardian agrees that my child and I shall comply with all documented terms and acknowledges that my child will be able to access the Internet via this device.

### Terms of Agreement

I hereby agree to the above statements. I also understand that my right to the use and possession of the property terminates the last calendar day of the current school year, unless terminated earlier by the school, or the student withdraws from the school division. I also understand that if the property is not returned the last day of classes, it will be considered stolen.

Parent/Guardian Signature \_\_\_\_\_ Date \_\_\_\_\_

Optional Insurance: ☐ I will purchase the optional accidental protection plan for \$33.  
☐ I am NOT purchasing the optional accidental protection plan and will be responsible for up to the full repair or replacement value if necessary.

**\*This form must be completed in its entirety in order to receive tablet.**

Date Received \_\_\_\_\_ ☐ Insurance form ☐ Paid

# APPENDIX F

# Bring Your Own Device (BYOD)

---

## Student/Parent Guidelines for use of a Privately Owned Electronic Device

Starting with the 2014-2015 school year, Dinwiddie County Public Schools will allow secondary students in grades 6-12 to use privately owned electronic devices to access the DCPS wireless network. This wireless access provided to the devices is designed to enhance the students' educational experience and outcomes. Connecting to the DCPS Wi-Fi network with personal devices is a privilege, not a right, and *it is not a requirement* for division students. Permission to bring and use privately owned devices is contingent upon adherence to DCPS guidelines. If a privately owned device is used by a student to disrupt the educational environment, that student's privileges may be limited or revoked.

### Guidelines

1. Students may use a privately owned electronic "Internet ready" device, including cell phones, on the DCPS wireless network with teacher or administrator permission for instructional purposes. The unauthorized use of cellular phones (calling or texting) is strictly prohibited.
2. Students may use devices on a school bus if permission is granted by the bus driver. The unauthorized use of cellular phones (calling or texting) is strictly prohibited. Voice, video, and image capture applications are prohibited on school buses.
3. Students are prohibited from accessing the Internet using any external Internet service, including the device's 3G or 4G capabilities.
4. No privately owned electronic device may be connected to the DCPS network by a network cable plugged into a data outlet. Network access is provided via Wi-Fi access only.
5. No student shall establish a wireless ad-hoc or peer-to-peer network using his/her electronic device or any other wireless device while on school grounds. This includes, but is not limited to using a privately owned electronic device as a cabled or wireless hotspot.
6. Voice, video, and image capture applications may only be used with teacher, staff or administrator permission.
7. Sound should be muted unless the teacher, staff or administrator grants permission for use of sound associated with the instructional activities. A teacher, staff or administrator may permit the use of ear buds or other types of headphones. Ear buds or other types of headphones must be provided by the student.

8. The privately owned electronic device owner is the only person allowed to use the device.
9. No division-owned academic or productivity software can be installed on personal devices.
10. No student shall use any computer or device to illegally collect any electronic data or disrupt networking services.
11. Devices are brought to school at the students' and parents' own risk. In the event that a privately owned device is lost, stolen or damaged, DCPS is not responsible for any financial or data loss.
12. Violation of school or division policies, local, state and/or federal laws while using a personal electronic device on the DCPS wireless network will result in appropriate disciplinary and/or legal action as specified in the *Student Handbook* and *Code of Student Conduct*, School Board policy as well as by local, state and/or federal law.
13. The school division assumes no responsibility for technical support. The school division and school division personnel cannot attempt to repair, correct, troubleshoot, or be responsible for malfunctioning personal hardware or software.
14. The student is expected to come to school each day with the personal device charged and ready to use.
15. The school division reserves the right to examine the privately owned electronic device and search its contents if there is reason to believe that school division policies or local, state and/or federal laws have been violated. In the event that a student believes that his/her password has been compromised, he/she should immediately reset his/her password using a school division computer.