



TECHNOLOGY & DIGITAL LEARNING PLAN

2017-2020

Collaborative Team

Dr. Tim Newman, Superintendent

Ms. Julie K. Christopher, Director of Technology

Dr. Shirlan Jenkins, Asst. Supt. - Curriculum & Instruction, Secondary

Ms. Penny Sturgill, Chief Academic Officer, Elementary

Mr. Stephen Watts, Digital Learning Coordinator

Orangeburg Consolidated School District 4

6080 Slab Landing Rd.

Cope, South Carolina 29038

(803) 534-8081

www.ocsd4sc.net

TABLE OF CONTENTS

District Profile	4
Executive Summary	5
Trends in K12 Education and Digital Learning	6
Student Learning and Classroom Technology	7-13
Assessment	7
Recent Progress	8
Goals and Objectives.....	8-10
Access 24/7/365.....	8
Digital Content & Courses.....	8
Equitable Access	9
Digital Literacy	9
Online Testing	9-10
Funding	11-12
Evaluation	13
Teacher and Employee Technology Tools	14-19
Assessment	14-15
Recent Progress	15
Goals and Objectives.....	16
Technology Proficiency	16
Equitable Access	16
Access to Digital Content	16
Technology Integration.....	16
Access to and Utilization of Student Data.....	16
Enhance Productivity	16
Funding	17-18
Evaluation	19
Safety and Security	20-23
Assessment	20
Recent Progress	21
Goals and Objectives.....	21
Physical Safety and Security.....	21
Virtual Security.....	21
Physical Data Security	21
Virtual Data Security	22
Funding	22-23
Evaluation	23

Infrastructure	24-29
Assessment	24-25
Recent Progress	26
Goals and Objectives.....	27
Sufficient Bandwidth.....	27
Reliable Wireless Access	27
Adequate Physical Environment.....	27
Functional Virtual Environment.....	27
Funding	27-28
Evaluation	29
Professional Development	30-33
Assessment	30
Recent Progress	31
Goals and Objectives.....	31-32
Enable Educators to Achieve/Demonstrate Proficiency	31
Provide Technology Leadership	31
Develop Certification Strands	32
Vary Delivery Methods	32
Funding	32-33
Evaluation	33
Technology Services	34
Assessment	34
Recent Progress	35
Goals and Objectives.....	35
Improve Quality & Timeliness of Service	35
Improve Provision of Data out of PowerSchool.....	35
Develop Process of New Technology Purchases.....	35
Provide Certification for Staff Members.....	35
Funding	36
Evaluation	37
Appendices	38-74
A - Technology Committee.....	38-39
B – Technology and Internet Acceptable Use Policy.....	40-52
C - South Carolina K-12 Internet Safety Standards	53-70
D - Refresh Cycle for District Office.....	71-72
E – Student & Parent Chromebook Agreement	73-74
References	75

DISTRICT PROFILE

Orangeburg Consolidated School District 4 (OCSD4) is one of three school districts located in Orangeburg, South Carolina. Orangeburg County, geographically the 2nd largest county in the state, covers over 1,100 square miles. A largely rural district (over 85% of the roads are unpaved), the county has approximately 90,000 residents of which 62% are African American and 35% are Caucasian. Orangeburg County is the home of Claflin University, South Carolina State University, and Orangeburg-Calhoun Technical College.

There are three school districts in Orangeburg County, with Orangeburg 4 serving the cities of Cope, Branchville, Cordova, Norway and Neeses. OCSD4 serves 20,430 residents in a 419 square mile rural area. 3,736 students attend 3 high, 3 middle, 3 elementary, 1 primary, and 1 alternative school. The Career Center serves students from OCSD4 and several neighboring counties. 3% of the population are ESL students; 6% are in the Gifted & Talented Program and 13% are Special Needs students. The district's free & reduced lunch rate is 100% (community eligibility) and eRate funding is currently at 85%. The demographics of each school is as follows:

School	Grades	Enrollment	Poverty Index	African-American	Caucasian	Hispanic	Other
Branchville Middle/High	6-12	349	54.3	28.7%	67.5%	.9%	2.9%
Carver Middle	6-8	523	74.7	42.5%	46.8%	5.1%	5.6%
Cope Area Career Center	9-12	527	52.7	40.4%	56.3%	NA	3.3%
Edisto Elementary	3-5	629	80.3	40.3%	49.5%	4.9%	5.3%
Edisto High	9-12	695	72.7	41.6%	51.6%	3.6%	3.2%
Edisto Primary	4K-2	698	82.3	45.6%	42.3%	5.7%	6.4%
HKT Elementary	4K-5	255	93.6	71.4%	23.3%	2.4%	2.9%
HKT Middle/High	6-12	276	90.4	77.9%	18.1%	2.2%	1.8%
Lockett Elementary	4K-5	298	66.2	27.6%	70.3%	0%	2.1%
STAR Center	6-8	56	NA	72.6%	23.3%	NA	4.1%

EXECUTIVE SUMMARY

The authors used the following documents as guidelines: *South Carolina State Educational Technology Plan (2014-2016)*, *The Horizon Report - 2016 K12 Edition*, *Maryland Technology Literacy Standards* for students and teachers, *ISTE Standards* for teachers and students, *2Revolutions Technology Combinations for Competency-Based Education*, and the *National Education Technology Plan 2016* (US Department of Education). Other contributors included the technology committee (comprised of teachers and staff from all schools - see Appendix A), site visits to neighboring districts and the Online Testing Technology Readiness Analysis Report compiled by Peak Performance for the South Carolina Department of Education.

This plan will use all the resources cited to articulate how OCSD4 will meet the six primary goals of the National Educational Technology Plan (NETP):

1. **Learning: Engage and Empower** - the district will provide all learners with engaging and empowering lessons that will make each student a lifelong learner and productive member of society
2. **Assessment: Measure What Matters** - OCSD4 will use technology to gather, assess and share data that will continue to assist teachers in making students academically successful
3. **Teaching: Prepare and Connect** - technology will be used to connect teachers in a timely and reliable way to the resources needed to provide an effective learning environment, including content, resources, and lessons
4. **Infrastructure: Access and Enable** - OCSD4 will provide a fast, solid, reliable infrastructure to students, teachers and staff, regardless of location or time of day
5. **Productivity: Redesign and Transform** - technology will be used as a vehicle for continuous improvement for the learning environment by making more efficient use of time and valuable resources
6. **Research and Develop: Innovate and Scale** - the district will continue to research highly effective practices that are successful in K12, higher education, and business to support all of the goals listed above

TRENDS IN K12 EDUCATION AND DIGITAL LEARNING

According to the *NMC/CoSN Horizon Report, 2016 K-12 Edition* the most important technological developments that will impact education are:

1. Markerspaces - a physical environment that fosters creativity and higher-order problem-solving
2. Online Learning - classes, programs and content available over the Internet
3. Robotics - designing and programming using hands-on learning
4. Virtual reality - computer-generated environment that simulates the physical presence of people and objects for more authentic learning
5. Artificial Intelligence - the creation of intelligent machines that would enhance learning and be able to respond intuitively to students
6. Wearable technology - smart devices in the form of jewelry, clothing, and eyewear that would allow classroom activities to encompass multidisciplinary efforts of design and programming

Some specific examples, cited by Mike Kennedy in *American School & University* magazine include:

- “Adaptive e-textbooks can detect the progress a student is making and alter the material that is presented subsequently to match the student’s mastery and learning style”.
- “Wearable technology contained in wristbands or embedded in clothing can monitor student activity and provide health and fitness data. Body cameras can transmit to the Internet what a student is seeing; virtual reality headsets immerse students in an interactive online experience”
- “Smart ID cards are embedded with technology that enables a school to take attendance automatically, lets students pay for a meal in the cafeteria or carry out other transactions, and borrow library books. They also bolster security by enabling schools to control access to a building or specific classroom”

As the District strives to provide personalized, virtual, blended, inquiry-based and competency-based learning to challenge and engage students, technology continues to evolve rapidly while funding remains scarce. OCSD4 is looking for creative ways to generate funding for technology including bond issuance, grant writing and re-purposing funds previously ear-marked for instructional materials and textbooks. The evolving trends listed above will continue to change how teachers teach and students learn.

STUDENT LEARNING AND CLASSROOM TECHNOLOGY

ASSESSMENT

There are three basic questions that the district needs to strategically answer in order to use digital tools to increase student achievement:

1. Technology integration - how is technology used to enhance and support student learning?
2. Digital curriculum - what technology skills do students need to learn and at what grade levels?
3. Digital citizenship - Are we teaching students to use technology in a responsible and appropriate way?

One of the biggest challenges is the [lack of Internet access](#) for students at home. In a recent survey conducted with 9-12 grade students via Chromebooks, 45.8% of high school students in OCSD4 do not have access to the Internet at home. Community organizations, especially churches are very willing to assist students by providing wireless access and a place to do homework. The district is looking for ways to foster these relationships.

Another challenge for integrating technology into the teaching and learning process is that there is not an easy-to-use, categorized portal available to OCSD4 teachers that contains [digital content](#) and lesson plans. Many of the OCSD4 teachers are reluctant to integrate technology in teaching because many think digital lesson plans have to be created from scratch. Teachers that have created digital content and lessons are willing to share but need a central location for storing and accessing.

Since the schools in the district are so diverse and geographically separate, not all students have [equitable access](#) to technology tools. The district needs to provide additional digital devices for ESL, gifted and talented, special needs, and general education (robotics, programmable hardware). Additional assistive devices are needed in order to meet the needs cited in all IEPs and 504s. A central repository would be a successful way to provide devices that can be checked out and re-used by all schools. Newer technology should also be available to students such as 3D printers, robotics, media walls, 3D, and so on. The district also needs to implement standard refresh rates for all hardware purchases.

Students are not [technology literate](#) or Internet savvy users, although many teachers believe so. Today's digital learners are not afraid to click on any icon, therefore they can get around easily. But what actual technology skills are students being taught such as creating a digital slide show, verifying the accuracy of data in a website, or creating a table in a document? The district needs to implement a technology proficiency test and standards beginning in grade 2. Students also need to learn to use technology tools in a responsible and appropriate manner.

Another significant challenge is providing adequate bandwidth, servers, Internet access, and devices for [online testing](#). The district began ACT and EOC testing on individual devices this school year and will be testing online at all schools in the Spring of 2017.

RECENT PROGRESS

The most notable progress in the last year and a half has been a dedicated funding stream for technology in the form of a bond referendum. The following technology has been installed to enhance teaching, learning and student achievement:

1. Internet access at home
 - a. Placed two computers at a local church for students to do homework
 - b. Received a grant from SCDoe to provide HotSpots for 420 ninth through twelfth grade students without Internet access at home
2. Digital content
 - a. Implementing a learning management system (LMS), which goes live in August 2017
 - b. Installed a keyboarding application in 4K-5th grade schools
 - c. Upgrading web-hosting application (*SchoolFusion* to *SchoolWires*)
3. Equitable access
 - a. Media centers - OCSD4 funded a technology refresh for all media centers that included new student and administrative computers, flatbed scanner, document camera and portable projector
 - b. Elementary schools - 6 Android tablets with a charging station were placed in every 4K, 5K, 1st and 2nd grade classroom
 - c. High schools - Chromebooks were distributed to every 9th-12th grade student. The Chromebooks are etched and a proxy server was installed so that the Internet is filtered no matter where the student uses the device
4. Digital literacy - in progress
5. Online testing
 - a. Computer labs - computers were either replaced or upgraded to 4GB of RAM to support online testing
 - b. Provision of headphones for ESL students
 - c. Set up bandwidth shaping for Chromebooks to enable ACT & EOC testing

GOALS AND OBJECTIVES

1. Provide access to digital content 24/7/365 for all students, employees and eligible stakeholders
 - a. Identify community locations such as restaurants, churches, higher education institutions, municipal buildings, etc that can provide after-hour wireless access
 - b. Develop liaisons with Internet providers to offer discounted home access to all stakeholders
 - c. Provide a portal to a repository of digital content that makes it easy to search and offers filtering according to CIPA guidelines
 - d. Install wireless access on school buses for students to work on homework
 - e. Purchase wireless devices that can be checked out to homebound students without Internet access
2. Increase access to digital content for students
 - a. Offer students more choice in regards to their own learning
 - b. Expand distance learning between the three high schools - honors, electives, foreign language, and other choices
 - c. Expand access to online classes by increasing offerings in *Edgenuity* (online courses for credit recovery and intervention) and Virtual SC

3. All students will have equitable access to digital learning tools
 - a. Implement digital technology and content that will support ESL students
 - b. Expand access to assistive technology that meets the needs described in a student's IEP or 504 plan by purchasing an inventory of assistive devices
 - c. Provide expanded technology such as robotics and 3D for gifted and talented students
 - d. Ensure that every classroom has the digital learning tools needed for successful teaching and learning
 - i. Add a document camera in each classroom
 - ii. Provide Chromebooks to every 3rd-8th grade student (to remain in classroom)
 - iii. Provide touch Chromebooks to every 4K-2nd grade student (to remain in classroom)
 - e. Develop a refresh strategy so technology can be updated at least every 4 years
 - i. When students graduate - the Chromebook can be kept
 - ii. Use usage fees to replace Chromebooks
 - f. Provide access to specialized technology tools for specific subject areas
 - i. Robotics, Science kits, 3D printer, Probes
 - ii. Middle School science - USB microscope, x-ray illuminator, ultrasound
4. All students will demonstrate technology literacy by the end of eighth grade
 - a. Identify an assessment tool to measure technology literacy (pre & post assessments)
 - b. Develop a curriculum that identifies the skills students are to master beginning in Kindergarten (integration into curriculum)
 - c. Develop a plan that enables keyboarding skill development to be taught at all grade levels
 - i. Primary and elementary - once a week in lab
 - ii. Middle school in business class
 - iii. High school in business classes as needed
 - d. Create a technology fair for students in grades 3-12 to compete in areas such as robotics, multimedia, and technology literacy
 - e. Incorporate Internet safety standards (*see appendix C*) and review ACUP at the beginning of each school year that covers:
 - i. Digital citizenship
 - ii. Media literacy
 - iii. Cyber ethics
 - iv. Personal safety
5. Provide the technology and environment (*see Infrastructure section*) needed for students to be successful during online testing on mobile devices
 - a. Cache server for every 50 students
 - b. Charging stations in every high school
 - c. Provide bandwidth shaping (9 Mbps for teachers/staff; 5 for students and 2 for guests)
 - d. Block the "video streaming" category during on-line testing to reduce bandwidth issues

OCSD 4 ON-LINE TESTING PLAN

<u>Test</u>	<u>Year OCSD4 started online</u>	<u>Year test to be administered on mobile devices</u>
ACT	2017	2016-2017 (Chromebooks)
ACT Workkeys	2017	2016-2017 (Chromebooks)
SCREADY	2016	2016-2017 (Chromebooks/Tablets)
SCPASS	2016	2016-2017 (Chromebooks/Tablets)
ACCESS for ELLs	2017	2019-2020 (Chromebooks/Tablets)
EOCEP	2014	2016-2017 (Chromebooks)
SCNCSC	2015	NA
DRA2	2016	2019-2020 (Tablets)
myIGDIs	2016	2019-2020 (Tablets)
MAP	2013	2016-2017 (Chromebooks/Tablets)

FUNDING

2017-2018		
WAPs for homework centers (1a)	\$ 1,000	General
Digital content & assistive devices - ESL (\$10 * 105) (3a)	\$ 1,050	Bond
Digital content & assistive devices - SpEd (\$10 * 479) (3b)	\$ 4,790	Bond
Digital content/devices for all students (\$10 * 3779) (3a-d)	\$ 37,790	Bond
Digital content & devices for G & T (\$10 * 223) (3c)	\$ 2,230	Bond
Wireless access for Homebound (1e)	\$ 5,000	Bond
Technology literacy assessment tool (4a)	\$ 10,000	Bond
Chromebooks w/charging station - middle schools (3cii)	\$ 279,800	Bond
Document camera for each classroom (3di)	\$ 89,375	Bond
Testing/caching servers at each school (1/50) [5a]	\$ 34,500	Bond
Wireless access on school buses (1d)	\$ 14,250	Bond
Replace 1-to-1 devices for senior class (3ei)	\$ 120,000	Bond
Internet access at home for 420 students without it (1a)	\$ 120,447	MoDAM grant
2018-2019		
Additional Edgenuity course content (2c)	\$ 20,000	Instruction
Chromebooks w/ charging station grades 3-5 (3dii)	\$ 317,525	Bond
Digital content & assistive devices - ESL (\$10 * 105) (3a)	\$ 1,050	Bond
Digital content & assistive devices - SpEd (\$10 * 479) (3b)	\$ 4,790	Bond

Digital content/devices for all students (\$10 * 3779) (3a-d)	\$ 37,790	Bond
Digital content & devices for G & T (\$10 * 223) (3c)	\$ 2,230	Bond
Technology literacy assessment tool (4a)	\$ 10,000	Bond
Replace 1-to-1 devices for senior class (3ei)	\$ 120,000	Bond
Wireless access on buses (1d)	\$ 8,500	Bond
2019-2020		
Touch Chromebooks w/ charging station for 4K-2 (3diii)	\$ 283,875	Bond
Digital content & assistive devices - ESL (\$10 * 105) (3a)	\$ 1,050	Bond
Digital content & assistive devices - SpEd (\$10 * 479) (3b)	\$ 4,790	Bond
Digital content/devices for all students (\$10 * 3779) (3a-d)	\$ 37,790	Bond
Digital content & devices for G & T (\$10 * 223) (3c)	\$ 2,230	Bond
Technology literacy assessment tool (4a)	\$ 10,000	Bond
Replace 1-to-1 devices for senior class (3ei)	\$ 120,000	Bond
Wireless access on buses (1d)	\$ 8,500	Bond

EVALUATION

1. Access 24/7/365
 - a. Student survey - administered annually
 - b. Teacher feedback
2. Access to Digital Content
 - a. Analyze content by grade and subject
 - b. Teacher feedback
3. Equitable Access
 - a. Teacher survey
 - b. Annual inventory
4. Technology Literacy
 - a. 8th grade assessment results
 - b. Keyboarding assessment scores
5. Online Testing
 - a. School feedback
 - b. Bandwidth usage

TEACHER & EMPLOYEE TECHNOLOGY TOOLS

ASSESSMENT

Students are motivated to use technology tools to explore, collaborate, solve, communicate, and learn at their own pace. The district is looking for ways to provide the support, training, and encouragement needed for teachers to embrace new ways of teaching and learning.

There is a large disparity between teachers, staff and employees in terms of [technology proficiency](#). Many users and some teachers still need basic technology and internet safety training. Basic technology proficiency would enable teachers to learn new applications much easier, such as *Canvas* and *MasteryConnect*. The district plans to purchase a technology proficiency test and administer to all teachers in 2017-2018. A professional learning plan (PLP) will be written for each teacher and re-certification credit awarded (see *Professional Development* section for additional information).

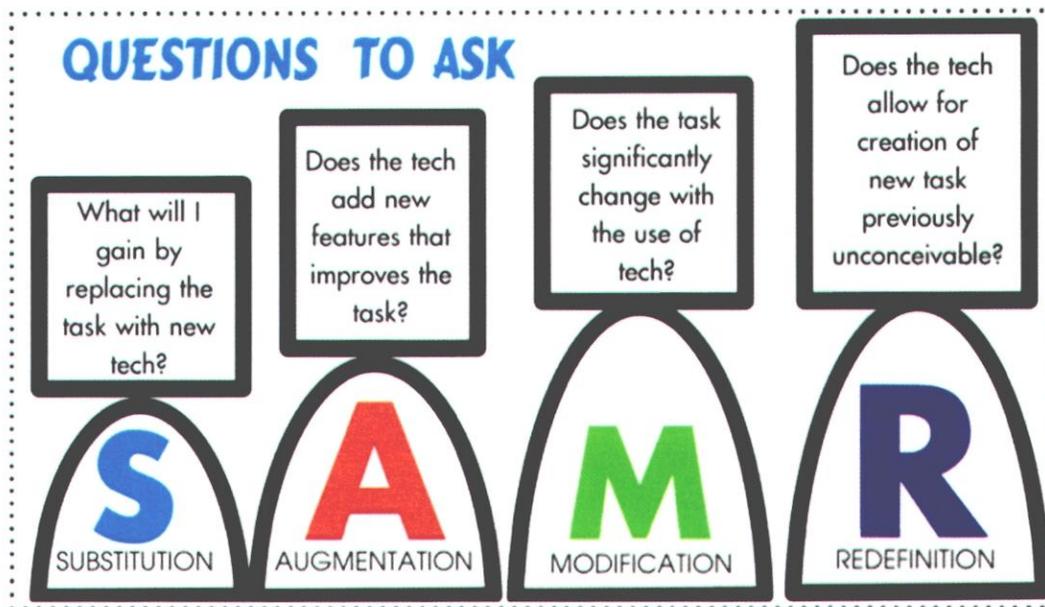
The district has made great strides in terms of [equitable access](#) to digital tools between schools and will continue to be mindful of equity. This plan will also establish refresh rate standards in order to maintain equitable access for students, staff and employees alike. During the installation of wireless interactive projectors, several classrooms already had inferior interactive boards and were skipped. This will be remedied during the summer of 2017. 4K-2nd grade and special education teachers received a touch whiteboard; 3rd-12th grade teacher whiteboards require a stylus. Teachers have requested that the touch module be added at these grade levels as well.

One of the biggest requests from teachers is [access to digital content](#) that is aligned to standards. The district is looking to provide a portal to organized digital content for all teachers based on grade level and subject area. The provision of a half-time Web Designer and half-time Grant Writer would achieve this purpose as well as locate additional funding for the technology cited in this plan.

The provision of [access to student data](#) for teachers is paramount, as the District implemented data teams in 2016-2017. The district is in the process of implementing a portal that will show teachers all available applications once they login to the portal. The application will use SSO so that teachers only need to login once and then click on applications that contain student data such as *MasteryConnect*, *Canvas*, *ENRICH* and *PowerSchool*. The district is also planning to implement a document server for *PowerSchool*, which will house all information about each student.

More employees need access to enhanced technology such as dual monitors in order to [enhance productivity](#). The plan to connect Active Directory (AD) to Google will greatly enhance the productivity of the technology staff, who are currently keeping multiple student and teacher databases up-to-date. The implementation of a portal for single sign-on (SSO) for employees and students will eliminate the time spent looking for passwords and emailing companies for password resets. Also, the implementation of a 4-year recycle plan will ensure that devices remain operable and fast (see *district refresh cycle in Appendix D*).

Another challenge is [technology integration](#) into the teaching and learning process. Many teachers are only using technology in the classroom as a “substitute”, based on the SAMR Model developed by Ruben Puentedura. Teachers continue to request hands-on classroom assistance with digital technology during the teaching process. Teachers have also asked to be paired with other teachers and see a model classroom in action.



RECENT PROGRESS

The most notable progress in the last year and a half has been a dedicated funding stream for technology in the form of a bond referendum. The following technology has been installed to enhance teaching, learning and student achievement:

1. Technology proficiency (work in progress)
2. Equitable access
 - a. Laptop for every teacher/administrator
 - b. New computer for every support position (guidance, secretary, bookkeeper)
 - c. Tablet for every 4K, 5K, 1st and 2nd grade teacher
 - d. Chromebook (touch screen) for every 9th-12th grade teacher
3. Access to digital content & standards
 - a. Provided access to *HMH* (digital textbooks)
 - b. Implementing *My Pathways*
4. Technology integration
 - a. Implementing learning management system (LMS) - *Canvas*
 - b. Hired a Digital Learning Coordinator
 - c. Installed *Hapara* to assist teachers with classroom management
5. Access to student data - Implementing *MasteryConnect*
6. Enhance productivity
 - a. Interactive projector in every classroom
 - b. New computers in Technology Training Center
 - c. Installed a flatbed scanner and new computers in each media center
 - d. Updated computers and peripherals for Parenting and Special Education employees

GOALS AND OBJECTIVES

1. All teachers will demonstrate technology proficiency
 - a. Subscribe to an on-line teacher proficiency test
 - b. Identify technology standards, create individualized plans, and monitor progress to certify all employees as technology proficient
 - c. Reward teachers who obtain proficiency
2. Equitable access to technology tools for all teachers
 - a. Replace non-touch interactive whiteboards with touch
 - b. Add the touch module to already installed projectors in grades 3-12
 - c. Implement *Clever* as a portal for SSO
 - d. Implement teacher mobile device management (MDM) application (*Hapara*) at all schools
 - e. Refresh teacher laptops
 - f. Provide licenses for whiteboard application
3. Digital content will be developed and shared across all grade levels and curriculum
 - a. Organize digital learning teams (DLTs) that meet regularly to develop and share lesson plans and digital content
 - b. Use the LMS to provide access to content and lessons that teachers are willing to share
 - c. Make blogging about and sharing content easily accessible
 - d. Research and link external content that is already aligned to standards and accessible for free (*Google for Education*, *SMART Exchange*, *SchoolTube*, and so on)
 - e. Eliminate the use of textbooks by 2020
 - f. Ensure that digital content includes various lessons that meet the learning modalities of each student
 - g. Hire a Web Designer/Grant Writer
4. Continue to provide the support teachers need to successfully integrate technology into teaching and learning when students are using mobile devices
 - a. Set-up separate SSIDs for students, teachers and guests
 - b. Provide dedicated bandwidth on WAPs for teachers and students
 - c. Hire certified teachers at every school to serve as Digital Literacy coaches
 - d. Hire another Digital Learning Coordinator to serve elementary and primary teachers
 - e. Adopt ISTE standards for teachers and create an integration rubric/standards-based tool for principals to use to evaluate integration & measure the effectiveness of technology infusion
5. Enhance usage of *PowerSchool* for data mining and reporting
 - a. Upgrade to the latest version
 - b. Integrate *PowerSchool* with Active Directory
 - c. Install a document server and create student portfolios to warehouse documents
 - d. Install and train teachers on the new *PowerTeacher Pro* gradebook
 - e. Add school lunch module to *PowerSchool*
6. Provide enhanced technology tools for employees to increase productivity
 - a. Automate teacher sign-in via the network
 - b. Automate school dismissal
 - c. Create a 3-4 year refresh cycle for all employees
 - d. Provide licenses for *Microsoft Productivity Suite*

FUNDING

2017-2018		
Consulting fees - SSIDs/WAPs configuration (4a & b)	\$ 10,000	Local
Mobile Device Management application for teachers (2d)	\$ 25,000	Bond
Replace TeamBoards with Epson interactive (2a)	\$ 62,000	Bond
Add touch module to 3 rd -12 th grade projectors (2b)	\$ 43,875	Bond
Technology proficiency assessment tool (1a)	\$ 10,000	Local
Automate school dismissal (6b)	\$ 5,000	Bond
<i>SMART Notebook</i> license renewal - annual (2f)	\$ 800	Local
<i>Microsoft Productivity Suite</i> license renewal - annual (6d)	\$ 28,300	Local
Web conference application for distance learning	\$ 501	Local
Parent notification application license	\$ 9,100	Local
2018-2019		
Continue <i>Canvas</i> subscription (3b)	\$ 25,000	Instruction
Digital Learning Coordinator (elementary/primary) (4d)	\$ 85,000	Local
Technology literacy assessment tool (1a)	\$ 10,000	Bond
Mobile Device Management license for teachers (2d)	\$ 25,000	Bond
Certificated teacher in each school to provide digital learning coaching (4c)	\$ 765,000	Unknown
Install <i>PowerSchool</i> document server (5c)	\$ 8,000	Bond
Web Designer/Grant Writer (3g)	\$ 60,000	Unknown
Automate school dismissal (6b)	\$ 5,000	Bond

<i>SMART Notebook</i> license renewal - annual (2f)	\$ 800	Local
<i>Microsoft Productivity Suite</i> license renewal - annual (6d)	\$ 28,300	Local
Web conference application for distance learning	\$ 501	Local
Parent notification application license	\$ 9,100	Local
2019-2020		
Continue <i>Canvas</i> subscription (3b)	\$ 26,000	Instruction
Replace teacher laptops (2e)	\$ 176,800	Bond
Digital Learning Coordinator (elementary/primary) (4d)	\$ 85,000	Local
Technology literacy assessment tool (1a)	\$ 10,000	Bond
Mobile Device Management license for teachers (2d)	\$ 25,000	Bond
Certificated teacher in each school to provide digital learning coaching (4c)	\$ 765,000	Unknown
Automate teacher sign-in - RFID on badge	\$ 5,000	Bond
Automate school dismissal (6b)	\$ 5,000	Bond
<i>SMART Notebook</i> license renewal - annual (2f)	\$ 800	Local
<i>Microsoft Productivity Suite</i> license renewal - annual (6d)	\$ 28,300	Local
Web conference application for distance learning	\$ 501	Local
Parent notification application license	\$ 9,100	Local

EVALUATION

1. Teacher technology proficiency - annual evaluation of assessment data
2. Equitable access to technology - Annual SDE inventory
3. Digital content development and sharing
 - a. Website usage statistics
 - b. Teacher feedback
4. Integration of technology
 - a. Review of rubrics
 - b. Principal survey
5. Enhance *PowerSchool* - user surveys
6. Enhanced productivity
 - a. Employee survey
 - b. Track refresh cycles

SAFETY AND SECURITY

Safety and security of both data and human beings (employees and students) can be divided into two categories - physical and virtual. The [physical security](#) of employees and students includes proactive technology such as door access control and running background checks on visitors to keep the schools and buildings safe. Reactive technology includes security cameras that can provide footage and caller ID software for threats. The [virtual security](#) of employees and students is enhanced through firewalls, content filtering, IP range blocking, anti-virus/anti-malware and SPAM filtering. The [physical data security](#) includes locking the data center and closets, and providing limited access to main network devices such as switches and wireless access points. [Virtual data security](#) means keeping intruders from accessing the network and accessing individual data through the use of firewalls, data encryption and stronger passwords.

ASSESSMENT

In terms of [physical security](#), many schools are still using analog cameras that cannot provide useable images to catch perpetrators, due to excessive pixelation. The analog cameras are connected via coax cabling and are not accessible through the Internet. Students and employees are not required to wear ID badges (except at one school). Although it is a rural district and school populations are small, individuals in the building still need to be able to identify a student or employee. All of the schools still use 3COM phone systems that are not upgradeable and only 'used' telephones are available to replace broken ones.

An anti-virus application is installed and operational for [virtual security](#) however, with limited staff, the district is not able to monitor critical events and computers that need updates installed. This is a function that needs to be incorporated into the Help Desk Manager's job description. The same applies for the SPAM filter - the appliance provides detailed information about SPAM being blocked but the data needs to be analyzed in order to block junk mail before it comes into the district.

The district needs to immediately implement [physical data security](#) for the data center. The door needs a biometric lock and to be accessible by only two individuals. The wiring closets at all the schools are enclosed in a locked cabinet however, the key remains hanging in the door. This needs to be remedied as well. The data center location, security and environment are limited due to current district facilities. It requires focused effort to ensure that it remains physically secure.

There are still some vulnerabilities in terms of [virtual data security](#) that need to be addressed. The WDS servers are not in full operation so *Windows* updates are not occurring automatically. The district does not own an email archiving device (although emails are backed up offsite and off grid). Either an appliance needs to be purchased or the district needs to migrate to *Office 365* or *Google Business Mail*, which both provide archiving. Currently, users are not required to change passwords for email, *PowerSchool* or finance applications. 180-day password changes will be implemented in the summer of 2017, along with complexity requirements.

RECENT PROGRESS

The most notable progress in the last year and a half has been a dedicated funding stream for technology in the form of a bond referendum. The following technology has been installed to provide safety and security:

1. Physical safety & security
 - a. Installed Visitor ID system with background check in every school
 - b. Installed 3 cameras and DVR on every bus in fleet
 - c. Installed digital IP security cameras at each high school (to cover perimeter)
 - d. Provided appropriate electrical outlets in all computer labs and media centers
2. Virtual security
 - a. Replaced firewall with new version (enhanced security features)
 - b. Installed new dashboard which enables firmware updates to be scheduled regularly
3. Physical data security - as part of re-cabling each school, installed a lockable wiring rack for all switches
4. Virtual data security
 - a. Implemented an anti-SPAM appliance
 - b. Implemented a standardized hardware/software catalog so individuals can only purchase approved devices
 - c. Set-up two SSIDs so students can no longer access the network from a cell phone
 - d. Installed additional SSL certificates for ENRICH and PowerSchool

GOALS AND OBJECTIVES

1. Enhance physical security of students and employees - surveillance and access control
 - a. Replace all analog cameras with digital IP cameras connect via POE
 - b. Purchase ID badge system for each building and require ID badges for employees and students
 - c. Implement door access control to provide keyless entry for employees
 - d. VoIP - replace telephone system and place station set/headset in each classroom
 - e. Enable cellular dialing over the wireless infrastructure for schools without cell service
 - f. Install card swipe on buses for students
2. Provide virtual security for students and employees while online
 - a. Show evidence that safety is provided on the Internet - policy, procedures, training materials, annual audit
 - b. Revise IUP and ACUP bi-annually (2017, 2019)
 - c. Monitor anti-virus critical issues daily
 - d. Require *Windows* updates on all devices
 - e. Monitor SPAM appliance and block senders
 - f. Monitor dashboard for rogue devices
 - g. Coordinate audit of *Google for Education* management console
 - h. Implement SSO for teachers and students
3. Increase physical data security
 - a. Install biometric lock on the door to the Data Center
 - b. Conduct thorough analysis of existing generator and maintain/check monthly
 - c. Lock all MDF/IDFs and remove the keys - technician only access

4. Enhance virtual data security
 - a. Implement email archiving through an appliance or migrate to cloud-based
 - b. Active WDS servers for automatic *Windows* updates
 - c. Set-up new password requirements for all applications (require change, length, etc)
 - d. Hire a consulting firm to re-engineer the Data Center (virtualization/cloud-based)

FUNDING

2017-2018		
Install digital IP security cameras in all buildings (1a)	\$ 650,000	Bond
Purchase ID badge printing solution for students and employees (1b)	\$ 16,000	Bond
Implement integration of LDAP and SSO (consulting services) [2h]	\$ 5,000	Local
Re-engineer Data Center (including disaster recovery & backups) [4d]	\$ 25,000	Bond
Purchase and install VoIP telephone system (1d)	\$ 110,000	Bond
Enable cellular dialing over wireless (1e)	\$ 5,000	Bond
Biometric lock for data center (3a)	\$ 1,200	Local
Analysis of existing generator (3b)	\$ 1,000	Local
Hire consulting firm to perform an audit of <i>Google Management Console</i> (2g)	\$ 4,000	Local
Email archiving appliance	\$ 10,000	Bond
Visitor ID badge software licensing	\$ 5,850	Local
AntiSPAM appliance licensing - <i>Barracuda</i>	\$ 1,200	Local
AntiVirus application licensing - <i>Kaspersky</i>	\$ 13,800	Local
2018-2019		
Implement door access control solution for exterior doors (1c)	\$ 60,000	Bond
VoIP annual licensing and support (1d)	\$ 10,000	Local
ID badge annual licensing and support (1b)	\$ 2,500	Local

Email archiving appliance licensing	\$ 2,500	Local
Visitor ID badge software licensing	\$ 5,850	Local
AntiSPAM appliance licensing - <i>Barracuda</i>	\$ 1,200	Local
AntiVirus application licensing - <i>Kaspersky</i>	\$ 13,800	Local
2019-2020		
Card swipe on school buses (1f)	\$ 35,000	Bond
VoIP annual licensing and support (1d)	\$ 10,000	Local
ID badge annual licensing and support (1b)	\$ 2,500	Local
Email archiving appliance licensing	\$ 2,500	Local
Visitor ID badge software licensing	\$ 5,850	Local
AntiSPAM appliance licensing - <i>Barracuda</i>	\$ 1,200	Local
AntiVirus application licensing - <i>Kaspersky</i>	\$ 13,800	Local

EVALUATION

1. Physical safety & security
 - a. Analysis of background check positives
 - b. Data export of discipline referrals on buses (has declined)
 - c. Data export of discipline referrals in schools
 - d. Annual number of breaking and entering incidents
2. Virtual security
 - a. Annual number of USOC incidents
 - b. Total SPAM per month
 - c. Total number of critical virus incidents per month
3. Physical data security - monitoring
4. Virtual data security - monitoring

INFRASTRUCTURE

Infrastructure is arguably the most important part of technology - the fundamental building block. If the underlying structure is not secure, stable and strong - the hardware and software in use above it will be unreliable, slow and insecure. Infrastructure includes the firewall, core switching, switches and wireless access points that support data and voice transport. Each of these must be configured to prioritize traffic (voice, PowerSchool, testing), limit guest usage, and provide adequate bandwidth for employees and students alike.

ASSESSMENT

Currently, there is **sufficient bandwidth** for the needs of the schools however, when individual devices are added to grades 3-8, more bandwidth will be needed both at the school level and district level. In 2013, the FCC established a minimum bandwidth target of 100 kilobits per second (kbps). The goal for 2018 is 1 Mbps per student. Current bandwidth levels are as follows:

School	Grades	Enr.	One-to-One	Bandwidth to school	Per student	Projected Bandwidth for 1Mbps/student
Branchville Middle/High	6-12	349	2016	75Mbps*	.22	350Mbps
Carver Middle	6-8	523	2017	150Mbps	.29	500Mbps
Cope Area Career Center	9-12	527	2017	100Mbps**	.19	500Mbps
Edisto Elementary	3-5	629	2018	150Mbps	.24	600Mbps
Edisto High	9-12	695	2016	150Mbps	.22	700Mbps
Edisto Primary	4K-2	698	2019	150Mbps	.22	700Mbps
HKT Elementary	4K-5	255	2018-19	75Mbps*	.30	250Mbps
HKT Middle/High	6-12	276	2016-17	75Mbps*	.27	300Mbps
Lockett Elementary	4K-5	298	2018-19	75Mbps*	.25	300Mbps
STAR Center	6-8	56	2017	50Mbps**	.89	60Mbps

*Branchville shares a 150Mbps circuit with Lockett; HKT Elementary and Middle/High share a 150Mbps circuit.

The Career Center and STAR have a bandwidth allocation out of the district allocation. *The District has a 1GBPS circuit but Cope and Star are allocated out of that total.

If the district increases school bandwidth to support the FCC requirement, the district will need a 4.5Gbps circuit at the district office. These requirements will be compounded once the district implements VoIP and migrates all applications to cloud-based (district email, PowerSchool, ENRICH, and other applications that are going cloud-based).

As more schools implement one-to-one devices, it is imperative that each school has [reliable wireless access](#). An outside network engineering firm assists the district with establishing gateways and SSIDs with dedicated bandwidth. Currently, the district provides 9Kbps for employees; 5Kbps for students and 2Kbps for guests at one high school. This will be further implemented in the summer of 2017. Students are also not allowed to connect cell phones to the wireless, as it adversely affects instruction due to limited bandwidth to the Internet.

The project to install category 6 and 6a cabling in each school will be complete by June 30, 2017. Funding was not available to provide an [adequate physical environment](#) for the wiring closets. Each closet will need an uninterruptable power supply (UPS) with enough outlets and volt-amps for the switches therein. Many of the closets do not have air conditioning, which will cause an issue during the summer months when the A/C is turned off. There are several closet locations that also have leaks in the ceiling that need to be repaired.

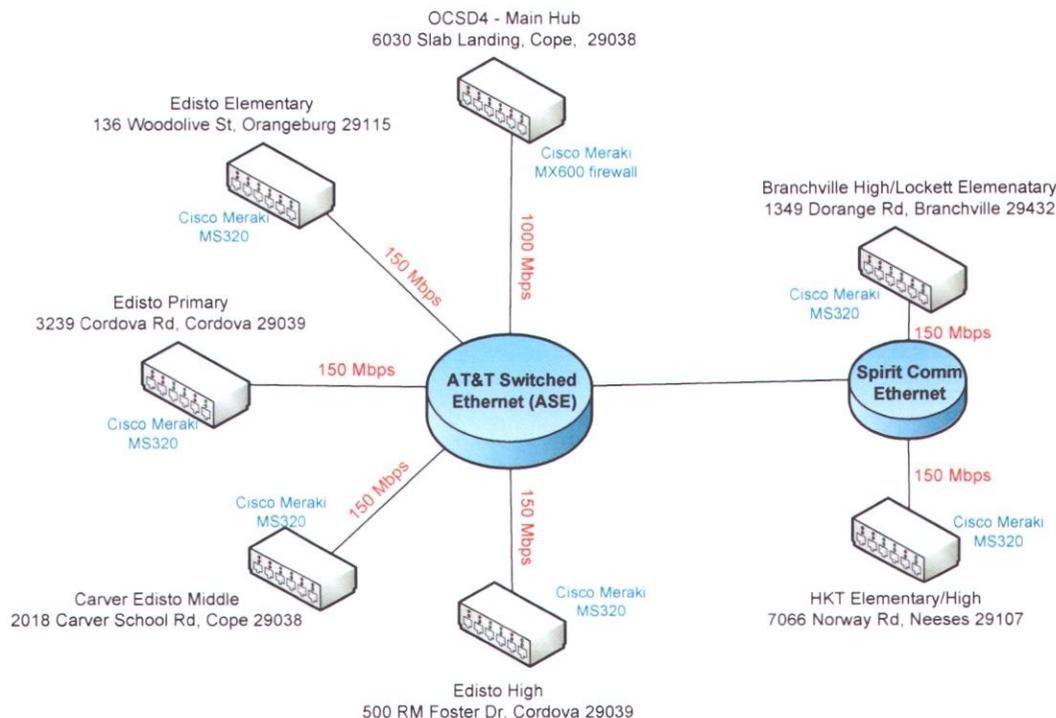
The servers and SANs in the data center currently do not provide a [functional virtual environment](#). Three of the oldest SANs need re-booting on a regular basis. All servers currently in use are EOL, as shown in the table below. The district has allocated funding in the bond issue to re-configure the data center. Vendors will be provided the opportunity to make recommendations for the district based on best practices. At this time, district technology personnel are leaning towards a hosted solution off-site, since there is not a suitable location for the data center.

<u>Brand</u>	<u>Model</u>	<u>Manufacture date</u>
Dell	PowerEdge 2950	February 2008
Dell	PowerEdge R720	May 2013
Dell	PowerEdge 2850	February 2006
Dell	PowerEdge R520	May 2013
Dell	PowerEdge R720	May 2013
Dell	PowerEdge R710	October 2009
Dell	PowerEdge R720	November 2012
Dell	PowerEdge R720	November 2012
Dell	PowerEdge R710	November 2009
Dell	PowerEdge R720	May 2013
Dell	PowerEdge 2950	June 2008
HP	MSA P2000 G3 storage array	September 2010
HP	MSA P2000 G3 storage array	September 2010
Dell	MD1000 PowerVault	May 2007

RECENT PROGRESS

The most notable progress in the last year and a half has been a dedicated funding stream for technology in the form of a bond referendum. The following technology has been installed to enhance the technology infrastructure:

1. Dedicated and sufficient bandwidth (see district diagram below)
 - a. The SDE increased the district bandwidth from 400Mbps to 1Gbps
 - b. The District is funding the increase of school bandwidth from 100Mbps to 150Mbps
 - c. By June 2017, all schools will be completely re-cabled using Cat 6 and Cat 6A cabling (10Gb backbone, 1Gb to desktop)
 - d. All switches have been replaced and are standardized
 - e. A new, larger firewall has been installed
2. Provide reliable wireless access
 - a. New wireless access points have been installed in every classroom
 - b. New wireless access points have been installed in all common areas such that each school is 100% wireless
 - c. Only three SSIDs will be available next year:
 - i. District (authenticates to AD)
 - ii. Students (limited by type of device)
 - iii. Guest
 - d. Each of the groups above have dedicated bandwidth as explained earlier
3. Ensure an adequate physical environment
 - a. New wiring racks have been placed in air conditioned spaces as much as possible
 - b. Additional electricity was added for most wiring cabinets
4. Provide a functional virtual environment - in progress



GOALS AND OBJECTIVES

1. Ensure dedicated and sufficient bandwidth
 - a. Work with network engineering consultant to provide dedicated bandwidth for high-priority applications such as *PowerSchool* and *Canvas*
 - b. Work with consultant to provide dedicated bandwidth within the school for intense users such as the principal, leadership, guidance
 - c. Re-allocate and monitor bandwidth when grades 6-8 get one-to-one devices
 - d. Re-allocate and monitor bandwidth when grades 3-5 get one-to-one devices
 - e. Proactively monitor bandwidth with network appliance
2. Provide reliable wireless access
 - a. Monitor access at each site weekly with a Wifi analyzer
 - b. Allow students to use the guest network on their cell phone as a guest only
3. Ensure an adequate physical environment
 - a. Provide adequate A/C in all wiring closets
 - b. Purchase a UPS for each wiring closet (with temperature monitoring)
 - c. Assess wiring closets for ceiling leaks and repair
4. Provide a functional virtual environment
 - a. Re-design data center to conform to best practices
 - b. Prepare disaster recovery plan
 - c. Prepare detailed backup plan
 - d. Replace existing web-hosting vendor

FUNDING

2017-2018		
Re-design Data Center (4a)	\$ 25,000	Bond
UPS in each wiring closet (3b)	\$ 50,000	Bond
Network engineering services (1a/1b)	\$15,000	Local
Increase 150Mbps to 500Mbps at middle and high schools (1c)	\$ 12,000	Local
Data Center backups - license renewal (annual) [4b]	\$ 3,300	Local
Cisco Meraki switches/WAPs licensing (annual)	\$ 70,000	Local
Virtual software licensing - <i>VMWare</i> (annual)	\$ 8,100	Local
AD management software licensing - <i>AD Manager</i> (annual)	\$ 1,500	Local
Webhosting license - <i>SchoolWires</i> (annual)	\$ 14,000	Local

2018-2019		
Increase 150Mbps to 500Mbps at elementary school (1c)	\$ 6,000	Local/eRate
Network appliance to proactively monitor bandwidth	\$ 15,000	Bond
Data Center backups - license renewal (annual) [4b]	\$ 3,300	Local
Cisco Meraki switches/WAPs licensing (annual)	\$ 70,000	Local
Virtual software licensing - <i>VMWare</i> (annual)	\$ 8,100	Local
AD management software licensing - <i>AD Manager</i> (annual)	\$ 1,500	Local
Webhosting license - <i>SchoolWires</i> (annual)	\$ 14,000	Local
2019-2020		
Increase 150Mbps to 500Mbps at primary school (1c)	\$ 6,000	Local/eRate
Network appliance to proactively monitor bandwidth	\$ 15,000	Bond
Data Center backups - license renewal (annual) [4b]	\$ 3,300	Local
Cisco Meraki switches/WAPs licensing (annual)	\$ 70,000	Local
Virtual software licensing - <i>VMWare</i> (annual)	\$ 8,100	Local
AD management software licensing - <i>AD Manager</i> (annual)	\$ 1,500	Local
Webhosting license - <i>SchoolWires</i> (annual)	\$ 14,000	Local

EVALUATION

1. Dedicated and sufficient bandwidth
 - a. Network monitoring appliance reports
 - b. Teacher survey
 - c. Dashboard switch analysis
2. Provide reliable wireless access
 - a. Weekly WiFi analyzer tests by technicians and make adjustments as needed
 - b. Teacher and student feedback (regarding response times)
3. Ensure an adequate physical environment - completion
4. Provide a functional virtual environment
 - a. Network uptime
 - b. Application response time
 - c. User feedback

PROFESSIONAL DEVELOPMENT

OCSD4 offers professional development through workshops, courses, seminars, help sessions, and individual user support. Research indicates that teachers may need as much as 50-80 hours to master new teaching strategies and concepts (French, 1997) and as much as 20 separate instances of using and practicing a skill before mastery (Joyce & Showers, 2002). Particular attention is given to present professional development in a manner that is relevant to the teachers and administrators, given content areas and grade levels. This is done either by discussions with staff prior to the event; needs assessments; or administrator requests.

ASSESSMENT

Currently, the district lacks a professional learning plan for teachers to [achieve and demonstrate integration of technology proficiency](#). During a casual walkthrough of classrooms, an observer might see one teacher walking around assisting individual students on their device; in another classroom you may see a teacher using a dry eraser marker on a whiteboard with the interactive projector off; in another, students using textbooks and posters taped in the projector space. Truly integrating technology is required to engage our 21st century digital natives.

Although the district now has a fulltime digital learning coordinator, there are over 250 teachers that need assistance with integration. The district has identified [technology leaders in each building](#) and needs to develop a model that trains these individuals to assist other teachers on a daily basis. Another strategy would be to subscribe to online training that teachers could take whenever and wherever, instead of relying solely on one person to deliver technology professional development.

The district does not typically [offer courses for specific groups](#) of users such as principals, guidance counselors, and administrative assistants. The majority of training is focused on classroom teachers. All employees would benefit from technology training on basic applications such as *Microsoft Excel*, *Google Productivity Suite* and *Outlook*. These courses would result in enhanced productivity for all employees.

Technology training is typically provided only as face-to-face. Employees need differentiation and a [variety of delivery](#) to stay engaged - just as students do. The district needs to explore and offer a variety of delivery methods such as webinars, self-paced modules, live webinars and even books for individuals that are comfortable with that format. Training for new applications such as *MasteryConnect* and *Canvas* could be outsourced to experienced, qualified instructors who could deliver training to the technology leaders in each building, who could in turn re-deliver. This would also help with the single point of failure - one DLC.

RECENT PROGRESS

The following progress has been made with regards to professional development:

1. Achieve and demonstrate proficiency
 - Last summer, all high school teachers attended 20 hours of integration training in preparation for the one-to-one initiative
 - Technology integration training is planned for middle school teachers at the end of the 2017 school year
2. Technology leadership
 - A Digital Learning Coordinator was hired in May of 2016
 - “Master” teachers were identified in 2015 and are providing training and assistance to other teachers in the building
3. Certification strands - in progress
4. Varied training - in progress

GOALS AND OBJECTIVES

1. Enable educators to achieve and demonstrate proficiency with integrating state recommended technology standards (ISTE) into their specific area of professional practice.
 - a. Create goals-based opportunities linked to teacher growth goals and district goals
 - b. Create a portfolio system that will assist teachers in demonstrating technology proficiency and integrating instructional technology into the classroom
 - c. Create a semi-annual survey to assess needs and progress
 - d. Create a diagnostic assessment so teachers and administrators can plan their learning and instruction more effectively
 - e. Create teacher learning plans that align with technology integration goals
 - f. Embed courses in the LMS so content is readily available to teachers
 - g. Consider ways to reward teachers for attaining higher levels, such as awarding badges within the LMS
 - h. Provide credits for re-certification, no matter how short the class is
2. Provide the schools with full-time, multi-dimensional technology leadership whose focus is to ensure that technology is making a significant, positive impact on both the instruction and administrative domains
 - a. Fund two, full-time digital learning coordinators (primary/elementary & middle/high) to assist teachers with developing, leading and evaluating technology integration into the classroom at all levels
 - b. Purchase more training from vendors as well as a subscription to online training (such as *Atomic Learning*). This will enable master teachers and digital learning coaches to provide direct training and consultation to teachers in their classrooms
 - c. Maintain a technology committee that provides input on decisions regarding technology procurement and professional development
 - d. Provide links to guidebooks and resources for teachers for all applications such as *MasteryConnect*, *Canvas*, and *PowerTeacher*

3. Develop certification strands for all groups of employees to encourage technology proficiency
 - a. Administration - *Microsoft Office* courses, *Classroom Mosaic*, *PowerSchool*
 - b. Teachers - *Microsoft Office* courses, *MasteryConnect*, *Canvas*, *SMART Notebook*
 - c. Classified - *Microsoft Office* courses, *Google Apps*
 - d. New Teachers - Logging in, *PowerTeacher*, *Exchange*, *ENRICH*
 - e. Technology Literacy and Responsible Use for all employees and students
4. Offer differentiation and varied methods of delivery
 - a. Foster collaborative opportunities with other districts, government, business, and higher education institutions who are willing to provide training to teachers
 - b. Provide self-paced courses, distance learning, virtual webinars and other formats that allow variety and flexibility for attendees and learners
 - c. Work creatively to outsource training so limited staff personnel can work individually with teachers and employees

FUNDING

2017-2018		
<i>Atomic Learning</i> subscription	\$ 10,000	State PD
Stipends for Digital Master Teachers	\$ 8,000	State PD
Professional training for individual applications	\$ 10,000	Bond
Stipends for teachers attending after-hours training	\$ 5,000	State PD
2018-2019		
<i>Atomic Learning</i> subscription	\$ 10,000	State PD
Stipends for Digital Master Teachers	\$ 8,000	State PD
Professional training for individual applications	\$ 10,000	Bond
Stipends for teachers attending after-hours training	\$ 5,000	State PD

2019-2020		
Atomic Learning subscription	\$ 10,000	State PD
Stipends for Digital Master Teachers	\$ 8,000	State PD
Professional training for individual applications	\$ 10,000	Bond
Stipends for teachers attending after-hours training	\$ 5,000	State PD

EVALUATION

The district will evaluate the success of Professional Development initiatives and the integration of technology in the classroom to improve student achievement as follows:

1. Achieve and demonstrate proficiency
 - Annual review of portfolios
 - Annual review of professional development plans
 - Individual class survey responses
2. Technology leadership
 - Teacher survey responses
 - Individual class survey responses
3. Certification strands
 - Individual class survey responses
 - Number of individuals that sign up for classes
4. Varied training
 - Employee survey responses
 - Assessment results from each session
 - Individual class survey results

TECHNOLOGY SERVICES

Technical support for all employees must be provided in such a manner as to not disrupt instruction. Conversely, technical support must be provided in such a manner as to ensure that *mode of instruction* is not disrupted - all student devices must remain operational and wireless access must work 100% of the time. Juggling the infrastructure for students and employees is one of the most challenging aspects of the technical staff's job. Another aspect is continuously reminding technicians that fellow employees are our customers, not just colleagues.

ASSESSMENT

As more devices are added to the network (over 1,200 added in 2017 alone), it becomes more challenging to [improve the quality and timeliness of service](#). And as more teachers integrate technology into instruction, they become dependent on reliable wireless access, the projector always working, and viable management software that continuously monitors. Although an additional technician was added to the staff this year (there are currently 3 technicians, a help desk manager, and the network manager), there were also 1200 Chromebooks added; a technician was re-assigned to the HelpDesk; and another technician became a full-time networking manager. Since staff is limited, finding ways to proactively monitor the network and bandwidth will assist the department greatly.

Principals have been asking for quite some time for the proactive [provision of data and reports out of PowerSchool](#). When data is needed, the principal must ask for the reports to be run or run the reports themselves. Typically, this is a reaction to a negative occurrence (parent complains there are no grades, student absences are excessive because a teacher wasn't taking attendance, etc). Providing this data weekly as a snapshot would assist principals with warning areas. Currently, the district only provides reports that are standard per the SDE. The district needs to provide additional training to the SIS coordinator so that custom reports can be generated.

Although there is standardized hardware and software catalog available, the district still needs to develop a [process for the purchase and implementation of new technology](#). The majority of the time, an end user purchases a software application and notifies technology that it needs to be installed. The technology department is not given the opportunity to evaluate the requirements, speak to the publisher about requirements, and understand the end user's needs. A formal process and requiring all requisitions to go through technology services would eliminate this issue.

The majority of the technical staff has not had professional technical training. The district needs to [provide training and certification](#) for the staff. Areas for training include: Cisco Meraki networking, *Google for Education*, Epson projectors, Dell computer/laptops, *Kasperky* Anti-Virus, *Mobotix*, and *vmWare* (to name a few). Additional funding will be needed to train each technician on a specific focus area. Some cross-training is needed as well to reduce the issue with single points of failure i.e. the individual that fixes Google issues is on vacation.

RECENT PROGRESS

1. Improve the quality and timeliness of service
 - a. Implemented full-time Help Desk support
 - b. Purchased remote control application for support
 - c. Added an additional technician
 - d. Made network manager responsible for staff closing tickets
2. Improve provision of data and reporting out of *PowerSchool* - in progress
3. Develop process for the purchase and implementation of new technology
 - a. Publish a hardware and software catalog quarterly
 - b. Increased communication with leadership team and principals
4. Provide certification for technical staff members
 - a. Trained staff on Mobotix IP cameras (vendor)
 - b. Trained staff on Cisco Meraki hardware (consultant)
 - c. Trained staff on *Kaspersky* anti-virus application (publisher)

GOALS AND OBJECTIVES

1. Improve the quality and timeliness of service
 - a. Purchase real-time network monitoring appliance tools (proactivity)
 - b. Establish on-going bi-monthly training for technical staff
 - c. Establish a metric for measuring response time and service
 - d. Explore apprenticeship program for students to become technicians
 - e. Work with high schools for students to provide 1st-tier support
 - f. Hire an administrative assistant for the department
 - g. Hire a dedicated technician for 1-to-1 schools
 - h. Train school-based personnel in basic troubleshooting skills
2. Improve provision of data and reporting out of *PowerSchool*
 - a. Send SIS manager to another district to learn how to customize reports
 - b. Send technician with *Sequel* training to another district to learn customization
 - c. Develop a dashboard for principals and guidance counselors with instant access to custom reports
3. Develop a process for the purchase and implementation of new technology
 - a. Develop a hardware acquisition request form for items not in the catalog
 - b. Develop a software acquisition request form
 - c. Develop a list of all information that will be required of the publisher for software approval
4. Provide certification for technical staff members
 - a. Basic networking protocols
 - b. *Google for Education*
 - c. Cisco Meraki hardware certification
 - d. Mobotix camera certification
 - e. *Clever* portal training
 - f. Additional *Kaspersky* training
 - g. *VMWare* certification

FUNDING

2017-2018		
IT ticket issuance and maintenance licenses - annual	\$ 3,000	Local
Survey tool - annual	\$ 300	Local
Remote access application - annual	\$ 340	Local
Cisco Meraki network certification	\$ 5,000	Local
VMWare certification	\$ 3,000	Local
Hire an administrative assistant	\$ 45,000	Local
Google for Education certification	\$ 5,000	Local
2018-2019		
IT ticket issuance and maintenance licenses - annual	\$ 3,000	Local
Survey tool - annual	\$ 300	Local
Remote access application - annual	\$ 340	Local
Hire an additional technician for VoIP, cameras, Chromebooks	\$ 55,000	Local
2019-2020		
IT ticket issuance and maintenance licenses - annual	\$ 3,000	Local
Survey tool - annual	\$ 300	Local
Remote access application - annual	\$ 340	Local

EVALUATION

1. Improve the quality and timeliness of service
 - a. Annual employee survey
 - b. Detailed analysis of trouble tickets opened/closed
2. Improve provision of data and reporting out of *PowerSchool* - Principal survey regarding *PowerSchool* reporting
3. Develop process for the purchase and implementation of new technology - adherence and feedback
4. Provide certification for technical staff members
 - a. Annual downtime
 - b. Analysis of trouble ticket turn-around time
 - c. Comparative study of consultant fees paid

APPENDIX A

The technology committee meets 6 times a year and includes the following individuals:

Branchville High	Merilyn Albergotti	Media Specialist
Branchville High	Elizabeth Tritapoe	Science
Branchville High	Wendy Morancie	Business Education
Cope Area Career Center	John Coleman	Automotive
Carver Middle	Sydnia Peterson	Science
Carver Middle	Trissie Kinsey	Media Specialist
Carver Middle	Allison Carson	Business Education
District Office	Julie Christopher	Director of Technology
District Office	Lois Preast	Help Desk Coordinator
District Office	Stephen Watts	Digital Learning Coordinator
District Office	Gina Edwards	Data & Testing Coordinator
District Office	Ron Stroman	Technician
District Office	Michael Holloway	Network Engineer
District Office	Curtis Huff	Technician
District Office	Wentsu Royster	Technician
Edisto Elementary	Amanda Looper	Math - 3 rd grade
Edisto Elementary	Caroline Robinson	Math - 4 th grade
Edisto Elementary	Cindy Hoover	Media Specialist
Edisto High	Lt. Colonel Davis	ROTC
Edisto High	Dr. Joni Jordan	Science

Edisto High	Adam Benson	Math
Edisto High	Wendy Metts	Media Specialist
Edisto High	Gregg Waters	Social Studies
Edisto Primary	Amy Thompson	Grade 2
Edisto Primary	Jennifer Moorer	Media Specialist
Edisto Primary	Kimberli Russell	Kindergarten
HKT Elementary	Valerie Funchess	Kindergarten
HKT Elementary/High	Gwendolyn Davis	Media Specialist
HKT Elementary	Veronica Wright	Computer Lab Aide
HKT High	Willette Williams	Science
HKT High	Aline Newton	English
HKT High	Marie Hallman	Social Studies
HKT Middle	Adrienne McMichael	Engilsh/Language Arts
Lockett Elementary	Jonsey Proctor	Gifted & Talented
Lockett Elementary	Rachel Cooper	Kindergarten
STAR	Brenda Martin	Business Education

APPENDIX B



TECHNOLOGY AND INTERNET ACCEPTABLE USE POLICY

Administrative Rule
10/21/03 & 4/22/2014

Issued 7/15/97; Revised

Computer technology and Internet access will be made available to all students attending Orangeburg Consolidated School District 4 (OCSD4) to promote educational excellence; to provide access to unique resources supplemental to the Media Center resources; to provide the opportunity for collaborative work; to stimulate personal growth in information-gathering, critical thinking and communication skills; to promote intellectual inquiry and awareness of global diversity through worldwide communication and exploration; and to assist students in developing the intellectual skills needed to discriminate among information sources.

District Rights and Responsibilities

It is OCSD4's responsibility to filter Internet access in accordance with the Children's Internet Protection Act (CIPA). OCSD4 reserves the right to deem what is appropriate and to access any and all data stored on computers, servers, school websites and in email to ensure that computer files do not contain defamatory, abusive, obscene, profane, sexually oriented, threatening, offensive or illegal material. The district also reserves the right to review any material downloaded or in use by any user and to deny an Internet or e-mail account to any student with a previous history of infractions related to computer use.

OCSD4 has no responsibility for the accuracy or quality of information obtained through the Internet. The availability of on-line resources does not indicate endorsement of contents by OCSD4.

User Rights and Responsibilities

Users represent the school district each time data is transferred over the Internet. All users must behave in an ethical and legal manner. Internet access is a privilege and with every privilege comes certain limitations and responsibilities:

- Using district-provided computers, laptops or other devices access for commercial activities, solicitation, fund-raising, charities, product advertisement/sales, or political lobbying is prohibited.
- The login account name and password given to each user becomes the user's responsibility. This information should not be shared with anyone else. If shared, the user will be responsible for any data transmitted under that user's account name.
- Users and guests may connect external devices to available wireless service provided by OCSD4 however, devices may not be physically connected to the network via cabling. The district will not be held liable for the theft of or damage to any device brought onto OCSD4 property.

Guidelines for use

OCSD4 will provide training to all students on appropriate computer and Internet use at the beginning of each school year. The following guidelines shall be followed by students when using the Internet/e-mail through the OCSD4 network:

- Users shall be polite, courteous and respectful during all sessions on the Internet/e-mail.
- Users must use appropriate language - profanity, obscenity or any vulgarity is prohibited.
- Users may not use another user's account name or password at any time.
- Users may not reveal their address, phone number, or other personal information about themselves, other students, teachers, administrators or colleagues via email or the Internet.
- Transmission of any material in violation of federal or state laws is prohibited (including but not limited to copyrighted, threatening, obscene or patent-protected material).
- OCSD will make every effort to control the content of data accessed through the Internet however there remains the possibility of a student discovering inappropriate material during a routine search. If this should occur, the user shall not share this information with any other student and shall notify the teacher immediately so this material can be filtered.
- If a student's use of the Internet, from any location including home, creates a likelihood of disruption (including threatening messages or violent websites) of school operation, the student may face school discipline and criminal penalties.
- Cyberbullying is defined by the National Crime Prevention Council as using the Internet or any other device to send/post text or pictures with the intention of hurting/embarrassing another person. Cyberbullying, whether generated at home or at school, is prohibited.

- Users are discouraged against using social networking sites such as Facebook for: derogatory comments related to students/staff; crude comments/references to sexual activity; photographs with nudity or near nudity; photographs/references to drug use, excessive alcohol use or drunkenness; potentially offensive commentary (race, disability, sexual orientation)

Violations

Students will be held accountable for violations of acceptable technology use. A student and his/her parent/guardian will also be responsible for damages and liable for costs incurred for service or repair. Violations of the Code of Conduct regarding the use of technology and the Internet include but are not limited to the following:

Level One Violations

- Deliberate search for or attempts to access inappropriate material
- Attempting to login to computers or use software as anyone other than yourself
- Plagiarism - *according to Merriam-Webster* is “to steal and pass off (the ideas or words of another) as one's own; use (another's production) without crediting the source; or to present as new and original an idea or product derived from an existing source”
- Misuse of computers for non-school related activities including gambling, shopping, online banking, personal transactions, and downloading of files (including but not limited to data, music, video, and games)
- Misuse of storage provided by the district by saving personal files without authorization such as journals, MP3s and game executable files

Level Two Violations

- Harassment of any user by persistent annoyance, bullying, intimidation, attempting to embarrass or the interference in another user's work or e-mail (sending of unwanted or duplicate e-mail is also defined as harassment)
- Creation of personal portals, web pages, music or game servers, or any other hosting device on school-owned equipment to store or share files such as music (MP3s for iPods), videos, games or any other file/application
- Downloading and/or installation of freeware, shareware, or application software
- Using websites, software, flash drives, fake wallpaper or any other method to create proxy servers to bypass OCSD4's Internet filtering application
- Theft of any computer or technology device owned by OCSD4 or someone else
- Sabotage or deliberate destruction/alteration of software applications, operating systems, or computer files

Level Three Violations

- Distribution of copyrighted software (software piracy is a federal offense punishable by fine or imprisonment)
- Vandalism including any malicious attempt to erase, modify or destroy the data of another user and the creation or uploading/downloading of computer viruses
- Electronic distribution of inappropriate material (games, music, videos, pornography)

- Electronic distribution of inappropriate material of a defamatory, obscene, abusive, offensive, profane, threatening, or hateful nature
- Engaging in any illegal activity electronically

Levels of Access

The district uses a filtering device that blocks websites by category. The determination of which websites that will not be allowed in a certain category are determined by a team of experts at the company that provides the filter. The district can however allow/disallow individual websites as requested by employees. Students, faculty and staff will be provided different levels of access as follows (blank cell denotes **Allowed**; shaded cell denotes **Blocked**):

<u>Category</u>	<u>Description</u>	<u>Students/Classroom</u>	<u>Teachers</u>	<u>Teachers 3pm-8am</u>	<u>Administration</u>	<u>Vocational Classes</u>	<u>Media Center</u>
Abortion	Abortion topics, either pro-life or pro-choice.						
Abused Drugs	Discussion about illegal, illicit, or abused drugs & "legal highs"						
Adult and Pornography	Sexually explicit material, adult products, online groups, etc						
Alcohol and Tobacco	Sites that support the sale of alcoholic beverages or tobacco						
Auctions	Sites supporting the offer/purchase of goods between individuals						
Bot Nets	Sites that are part of a Bot network (launches network attacks)						
Business and Economy	Business/corporate, econ, mkting, mgmt & entrepreneurship						
Cheating	Sites that support cheating & contain plagiarized documents						
Computer and Internet Info	General computer and Internet sites, technical information						
Computer and Internet Security	Computer/Internet security, security discussion groups						
Content Delivery Networks	Delivery of content/data (ads, media, files, images, and video)						
Cult and Occult	Astrology, spells/curses, magic powers, horoscopes, etc						
Dating	Dating websites focused on establishing personal relationships						
Dead Sites	Sites that do not respond to http queries.						
Dynamically Generated Content	Content dynamically based on a web request						
Educational Institutions	Pre-school, K12, college, university, and vocational school sites						
Entertainment and Arts	Movies, TV, music, books, comics, performing arts, museums						
Fashion and Beauty	Fashion or glamour magazines, beauty, clothes, cosmetics, style						
Financial Services	Banking services not including brokerage or trading services						
Gambling	Gambling, lottery, virtual casinos, sports picks, fantasy leagues						
Games	Playing, downloading, selling, sweepstakes, giveaways						
Government	Govt agencies/services, sites that discuss or explain laws						
Gross	Vomit and other bodily functions, bloody clothing, etc.						
Hacking	Access/distribution of apps to allow compromise of networks						
Hate and Racism	Support content for hate crimes and racism						
Health and Medicine	General health, fitness, well-being, medical information						
Home and Garden	Home issues & products such as decor, cooking, gardening, etc						

Category	Description	Students/Classroom	Teachers	Teachers 3pm-8am	Administration	Vocational Classes	Media Center
Illegal	Criminal activity, how not to get caught, copyright violations, etc						
Hunting and Fishing	Sport hunting, gun clubs, and fishing						
Image and Video Search	Photo/image searches, photo albums/exchange, image hosting						
Individual Stock Advice and Tools	Stock trading, mgmt of assets, investment strategies, quotes						
Internet Communications	Internet telephony, messaging, VoIP services and related						
Internet Portals	Aggregate a broader set of Internet content and topics						
Job Search	Assistance in finding employment or looking for employees						
Keyloggers and Monitoring	Software that track keystrokes or monitor web surfing habits						
Kids	Sites designed specifically for children and teenagers						
Legal	Legal websites, law firms, discussions/analysis of legal issues						
Local Information	City guides, tourism, restaurants, area/regional information						
Malware Sites	Malicious content (exe files, scripts, viruses, trojans, and code)						
Marijuana	Marijuana use, cultivation, history, culture, legal issues						
Military	Military branches, armed services, and military history						
Motor Vehicles	Cars/trucks/boats/RV reviews, sales tips, parts catalogs, trading						
Music	Music sales, distribution, streaming, lyrics, performances						
News and Media	Current events, radio, magazines, newspapers, weather sites						
Nudity	Nude or seminude depictions of the human body						
Online Greeting cards	Online Greeting card sites						
Parked Domains	Host pass-thru ads that don't contain content useful to the user						
Pay to Surf	Pay users cash/prizes for reading links, email, web pages						
Peer to Peer	Peer to peer clients/access, torrents, music download programs						
Personal sites and Blogs	Personal websites posted by individuals/groups & blogs						
Personal Storage	Online storage/posting of files, music, pictures, and other data						
Philosophy and Political Advocacy	Politics, philosophy, promotion of a viewpoint to further a cause						
Phishing and Other Frauds	Phishing/pharming to harvest personal information from a user						
Proxy Avoidance/Anonymizers	Proxy servers to bypass website filtering or monitoring						
Questionable	Tasteless humor, "get rich quick", manipulation of user experience						
Real Estate	Renting, buying, or selling real estate/properties.						
Recreation and Hobbies	Collecting things, models/kits, outdoor activities, pets						
Reference and Research	Personal, professional, or educational reference materials						

<u>Category</u>	<u>Description</u>	<u>Students/Classroom</u>	<u>Teachers</u>	<u>Teachers 3pm-8am</u>	<u>Administration</u>	<u>Vocational Classrooms</u>	<u>Media Center</u>
Shopping	Stores, catalogs, online shopping						
Religion	Religious subjects, houses of worship						
Search Engines	Sites using key words to find text, websites, images, videos, files						
Sex Education	Reproduction, safe sex, diseases, tips, contraceptives						
Shareware and Freeware	Software, screensavers, icons, wallpapers, utilities, ringtones						
Social Networking	Communities where users interact, post messages/pictures						
Society	Broad issues groups/associations (safety, children, philanthropy)						
SPAM URLs	URLs contained in SPAM						
Sports	Teams, conferences, scores, schedules, magazines						
Spyware and Adware	Data gathering that is unknown to the user (includes popups)						
Streaming Media	Sales, delivery, streaming of audio or video content						
Swimsuits & Intimate Apparel	Swimsuits, intimate apparel or other types of suggestive clothing						
Training and Tools	Trade schools, online courses, vocational training						
Translation	Language translation but may allow users to circumvent filtering						
Travel	Airlines, travel, car rentals, promotions for hotels/casinos						
Violence	Advocate violence/methods incl. game/comic violence, suicide						
Weapons	Sales/reviews of weapons						
Web Advertisements	Advertisements, media, content, and banners						
Web based email	Sites offering web based email and email clients						
Web Hosting	Free/paid hosting services for web pages						

*** THIS FORM MUST BE RETURNED FOR YOUR STUDENT TO USE COMPUTERS ***

Elementary Student Computer Use Contract

My parents and I have discussed the use of computers at school and I, [*print*] _____, agree to the following:

- I will only use the computer with an adult in the room.
- I know that misuse of the computer could lead to serious consequences.
- I will not share any personal information such as name, address, or phone number of my parents, classmates, teachers or anyone else over the Internet.
- I will not give my account name or password to any other student or use another student's login.
- I understand that my parents will have to pay for anything that I break, destroy or steal.

Signed _____ Dated _____

Parent/Guardian Consent Form

In Orangeburg Consolidated School District 4 (OCSD4), your child has access to computers and the Internet. It is important that you and your child read the Internet Use Policy included in the Code of Conduct **together**, as inappropriate use will result in disciplinary action.

I, [*print*] _____, the parent/guardian of the above student, agree to accept all legal and financial obligations which may result from my child's use of OCSD4 computers and the Internet. I also understand that I am liable for any damages incurred from theft or defacing of school property.

As the parent/guardian of this student, I have read the Internet Use Policy. I understand that access is designed for educational purposes and that OCSD4 has taken all available precautions to eliminate controversial materials. I will not hold the school system responsible for inappropriate materials acquired through the Internet. Further, I accept full responsibility for the actions of my child.

I grant permission for my child to use computers and the Internet as provided by OCSD4.

Yes No

I grant permission for my child to use an e-mail account at school for instructional purposes only.

Yes No

I grant permission for the publication my child's creative work on the school website. No home address or telephone number will appear with such work. His/her name may be published with the work.

Yes No

I grant permission for my child's name and photograph to be published on a School District website.

Yes No

Signed _____ Dated _____

***** THIS FORM MUST BE RETURNED FOR YOUR STUDENT TO USE COMPUTERS *****

Secondary Student Computer Use Contract

My parents and I have discussed the use of computers at school and I, *[print]* _____, agree to the following:

- I will abide by all computer rules and regulations stated in the Code of Conduct.
- I understand that inappropriate use will lead to penalties including but not limited to the loss of my account and disciplinary or legal action.
- I will not share any personal information such as name, address, or phone number of my parents, classmates, or teachers over the Internet.
- I will not give my login or password to any student or use another student's login.
- I understand that my parents will have to pay for any computer or electronic equipment that I break, destroy, or steal.

I release Orangeburg Consolidated School District 4 (OCSD4) from any liability or damages that may result from my use of the Internet or computers, either financially or legally. I acknowledge that safe guards are in place to limit my access to inappropriate Web resources.

Signed _____ Dated _____

Parent/Guardian Consent Form

In OCSD4, your student has access to computers, the Internet and other electronic resources. It is important that you and your child to read the Internet Use Policy in the Code of Conduct together. Inappropriate use will result in disciplinary action.

I, *[print]* _____, the parent/guardian of the above student, agree to accept all legal and financial obligations which may result from my child's use of OCSD4 computers and the Internet. I also understand that I am liable for any damages incurred from theft or defacing of school property.

As the parent or guardian of this student, I have read the Internet Use Policy in the Code of Conduct. I understand that this access is designed for educational purposes and that OCSD4 has taken all available precautions to eliminate controversial materials. I will not hold the district responsible for inappropriate materials acquired through the Internet. Further, I accept full responsibility for the actions of my child.

I grant permission for my child to use computers and the Internet as provided by OCSD4.

Yes No

I grant permission for my child to use an e-mail account for instructional purposes only.

Yes No

I grant permission for publication of my child's creative work on the school website. No home address or telephone number will appear. His/her name may be published with the work.

Yes No

I grant permission for my child's name & photograph to be published on a OCSD4 website.

Yes No

Signed _____ Dated _____

EMPLOYEE ELECTRONIC MEDIA USE POLICY

Technology, Internet access and the e-mail system are the sole property of Orangeburg Consolidated School District 4 (OCSD4) and are provided for the purpose of fulfilling district goals. The purpose of this policy is to provide guidelines and to assist users in determining appropriate use of district-owned technology. Noncompliance with this policy may result in discipline up to, and including, termination and/or criminal prosecution.

Computer Configuration

Technology (computers, laptops, smartphones, etc) that accesses the network, e-mail and Internet in the district is configured very differently from home computers. Users are provided access to files and services based on individual job descriptions. Certain configurations may seem constricting to the user, but are required for accessibility. Users therefore, may not install software or shareware, change operating system configurations, or install additional hardware without authorization from the Director of Technology. Users must take every step necessary to avoid introducing a destructive computer virus into the system.

Employees may connect external devices to available wireless service provided by OCSD4 however, devices may not be physically connected to the network via cabling. The district will not be held liable for the theft of or damage to any device brought onto OCSD4 property.

District Monitoring

OCSD4 reserves the right to access computer files, e-mail and Internet use logs as District Administration deems appropriate. Random monitoring of Internet usage will be done on a regular basis to monitor excessive or inappropriate use. Monitoring of a specific individual requested by a supervisor must be authorized by the Superintendent or designee and be based on reasonable suspicion of misuse or wrongdoing documented in writing.

Software Copyright

OCSD4 does not own computer software, but rather licenses the right to use software. Unauthorized copying, redistributing, or republishing of copyrighted or proprietary material is prohibited and is a violation of state and federal law. Users may not install software from home or other outside sources, and may not download it from the Internet to district-owned devices. OCSD4 will work diligently to provide the appropriate software applications for employees to successfully do their job.

Password Selection and Usage

All users must utilize a password to access the network and e-mail system. Passwords are confidential and should not be shared with anyone. Sharing a password could provide a user access to confidential information that could be altered or deleted. The following guidelines should be used with reference to passwords:

- Passwords should be 5-8 characters in length and include both letters and numbers
- Do not use passwords containing information that is public (spouse name, hobbies, interests, child's names, birthday, etc)
- Do not provide your password to anyone or send your password through email
- Do not write your password down where it can be easily found or identified
- Passwords cannot be recovered if forgotten but can be changed. It is the responsibility of each user to remember passwords to the network, e-mail, etc.
- Employees should take care to logout of sensitive applications such as *PowerSchool* and *Outlook* (email) when leaving the computer un-attended

Personal Announcements and Personal Projects

Using e-mail for personal announcements (birthdays, showers, weddings) and solicitations (fund-raisers for charities, schools, or church projects) is prohibited. Solicitation for an outside business such as Mary Kay or Avon is also prohibited. Jokes, chain letters, or any other non-business related materials should not be sent over OCSD4 e-mail.

Internet Access

Computers and Internet access will be made available to employees as needed for the performance of job duties. The following activities are prohibited:

- Downloading data, files, programs, pictures, pornography, jokes, screen savers, games, shareware, freeware, and attachments.
- Accessing the Internet for personal profit or gain
- Speaking on behalf of Orangeburg Consolidated School District 4
- Accessing inappropriate web sites
- Gambling or any other illegal activity
- Participation in chat rooms

E-mail Communications

E-mail messages may be read by someone other than the addressee and may even someday have to be disclosed to outside parties or to a court of law in connection with litigation. Accordingly, please take care to ensure that your messages are courteous, professional and businesslike.

The following e-mail activity is strictly prohibited:

- Accessing or trying to access another user's e-mail account
- Using e-mail to harass, discriminate, or make defamatory comments, even in a joking manner
- Using computers to store or transmit inappropriate jokes, junk mail, or chain letters
- Using e-mail to solicit for commercial, religious, charitable, or political causes
- Using e-mail to misrepresent or disparage OCSD4
- Using e-mail for personal gain
- E-mail should not be used in any way that may be insulting, disruptive or offensive to any other person (including sexually explicit messages or gender-specific comments; cartoons or jokes; chainletters; unwelcome propositions (romantic or otherwise); ethnic or racial slurs; or any other message that can be construed to be harassment or which addresses a person's sex, race, sexual orientation, age, national origin, religious or political beliefs or disability.
- Any and all data, including email that is stored on or sent through the OCSD4 network is subject to review. All documents created during an employee's tenure will remain the property of the district upon separation.

Sabotage

Any destruction or alteration of district computers, software applications, files, servers, or data (including deletion or unauthorized duplication) is prohibited. Offenders will be prosecuted to the fullest extent of the law or otherwise disciplined, including possible termination.

Computer and Internet Use Policy Agreement

I thoroughly understand the Computer and Internet Use Policy and agree to abide by all stated guidelines. I understand that I have a responsibility to report any violations of the policy. I also understand that OCSD4 reserves the right to monitor and disclose any e-mail or Internet records, with or without employee notice, and that monitoring may occur during or after working hours. I am aware that this signed agreement will be posted in my personnel file.

Employee Signature: _____ Date: _____

Employee Name (Please Print): _____

Location: _____

APPENDIX C

South Carolina K-12 Internet Safety Standards South Carolina Department of Education Columbia, South Carolina 2009 Standards Overview

Today's students, having grown up with technology and digital devices, are called digital natives. They are very technology savvy but still need instruction and guidance to become technology literate. Part of being technologically literate is knowing how to use technology effectively, responsibly, and safely. The South Carolina K-12 Internet Safety Standards were developed to provide a framework and guidance for educators as they work with their students to learn 21st Century skills and to become information and technologically literate.

The *National Education Technology Standards for Students* (NETS-Students) published by the International Society for Technology in Education (ISTE) and the national *Standards for the 21st Century Learner*, published by the American Association of School Librarians (AASL) address the issue of responsible use of information and technology. However, these standards do not address in-depth the issue of what students need to know in order to be safe in an online environment. The South Carolina K-12 Internet Safety Standards were written to fill this gap.

The South Carolina Department of Education (SCDE) CyberSafety Task Force was charged with developing a public awareness Internet safety program to design, develop, produce, and distribute instructional materials and programs for classroom teachers and administrators. These Internet Safety Standards are the basis for this public awareness program.

The standards are divided by grade bands—primary, elementary, middle, and high. The grade bands are as follows:

- [Primary](#): Kindergarten – Grade 2
- [Elementary](#): Grades 3-5
- [Middle](#): Grades 6-8
- [High](#): Grades 9-12

K-12 Internet Safety Standards

Standard 1: Students recognize their rights and responsibilities in using technologies within the context of today's world.

Standard 2: Students use critical thinking and evaluation while incorporating appropriate digital tools and resources into their education.

Standard 3: Students recognize the ethical and legal issues while accessing, creating, and using digital tools and resources in order to make informed decisions.

Standard 4: Students will recognize online risks and dangers in order to take appropriate actions to protect themselves while using digital tools and resources.

Primary (Kindergarten - Grade 2)

Digital Citizenship

Standard 1: Students recognize their rights and responsibilities in using technologies within the context of today's world.

Indicators:

1. Recognize that content uploaded to the web is accessible to everyone and creates a reflection of who you are throughout your life. - Students will recognize that various forms of content exist on the Internet.
2. Understand the difference between reality and virtual citizenship as it pertains to virtual games and virtual worlds - Students will recognize the difference between reality and virtual (real vs. unreal).
3. Exhibit responsibility, safety and etiquette when communicating digitally.
 - Students will recognize that various forms of communication exist (e.g., text messaging, email, blogging).
 - Students will be polite communicating
 - Students will communicate only in child-safe environments (e.g., ePals, eChalk, SharpSchools, Class Blogmeister).

Media Literacy

Standard 2: Students use critical thinking and evaluation while incorporating appropriate digital tools and resources into their education.

Indicators:

1. Recognize author bias, critically evaluate resources, and apply effective search practices when researching on the Internet.
 - Students will recognize that not all content on the Internet is true.
 - Students will use only teacher approved sites in a monitored environment.
2. Collaborate safely, responsibly, and effectively when using wikis, blogs, email, and emerging technologies.

Students will use collaboration tools (e.g., Google Docs, wikis, blogs) only with adult supervision.
3. Identify digital propaganda (e.g., pop up ads, spam).

Students will recognize the purpose of pop-up advertisements.

Cyber Ethics

Standard 3: Students recognize the ethical and legal issues while accessing, creating, and using digital tools and resources in order to make informed decisions.

Indicators:

1. Respect the copyright and intellectual property rights of others.

Students will understand that illegal downloading or copying resources is stealing.
2. Identify plagiarism when using digital tools and content.

Students will recognize that copying content directly from the Internet and claiming it as their own is stealing and against the law.
3. Identify hacking and recognize the legal ramifications.

Students will only use their personal login and password.
4. Understand the legal, ethical, and privacy guidelines for emailing and viewing/posting content.
 - Students will recognize that posting inappropriate pictures of themselves and others is wrong.
 - Students will recognize that sending inappropriate emails about others is wrong.

5. Recognize the responsibility, legal consequences, and emotional effects of cyberbullying.

Students will recognize that bullying online is the same as real life bullying.

Personal Safety

Standard 4: Students will recognize online risks and dangers in order to take appropriate actions to protect themselves while using digital tools and resources.

Indicators:

1. Recognize attempts at phishing for information.
Students will be taught not to open up email messages from people they do not recognize.
2. Implement procedures to protect computer systems from viruses and hackers.
Students will not open email attachments without adult supervision.
3. Recognize the tactics that online predators use to lure students.
 - Students will not talk to strangers online.
 - Students will tell an adult if someone online makes them feel uncomfortable.
 - Students will not give out any personal information (name, address, phone number, email address, school name, personal description, etc.).
4. Avoid access to controversial content.
Students will only go to sites that have been approved by an adult.
5. Avoid sharing personal logins and passwords.
Students will never tell anyone their personal login or password.
6. Identify the type of information that may lead to identity theft.
Students will not give out any personal information (e.g., name, address, phone number, email address, school name, personal description).
7. Identify the appropriate use and safety precautions when participating in online activities.
 - Students will not give out personal information online.
 - Students should only participate in chatrooms, instant messaging, social networking, and online games with the permission and supervision of an adult.

Elementary (Grades 3-5)

Digital Citizenship

Standard 1: Students recognize their rights and responsibilities in using technologies within the context of today's world.

Indicators:

1. Recognize that content uploaded to the web is accessible to everyone and creates a reflection of who you are throughout your life.
 - a. Students will use discernment when posting content on email, websites, social networks, wikis, blogs and other collaboration tools
 - b. Students will understand that Internet content can be archived and can exist forever.
2. Understand the difference between reality and virtual citizenship as it pertains to virtual games and virtual worlds.
 - a. Students will recognize the difference between reality and virtual (real vs. unreal)
3. Exhibit responsibility, safety and etiquette when communicating digitally.
 - a. Students will safely and responsibly use various forms of communication.
 - b. Students will recognize who has access to view and respond to communication.
 - c. Students will understand that online communication, including email and text messaging, is never private and may be shared with others without your knowledge.
 - d. Students will communicate politely in email, wikis, blogs, and forums.

Students should communicate only in child-safe environments (e.g., ePals, eChalk, SharpSchools, Class Blogmeister).

Media Literacy

Standard 2: Students use critical thinking and evaluation while incorporating appropriate digital tools and resources into their education.

Indicators:

1. Recognize author bias, critically evaluate resources, and apply effective search practices when researching on the Internet.

- Students will recognize that not all content on the Internet is true.
 - Students will use teacher approved sites and kid-friendly search engines in a monitored environment.
2. Collaborate safely, responsibly, and effectively when using wikis, blogs, email, and emerging technologies.
 - Students should use collaboration tools (e.g., Google Docs, wikis, blogs) only with adult supervision.
 - Students will learn to use appropriate collaboration tools and exhibit responsible behavior.
 3. Understand the appropriate time and place to use instant messaging lingo and emoticons as they apply to formal and informal writing.

Students will understand that instant messaging lingo is a part of informal writing.
 4. Identify digital propaganda (e.g., pop up ads, spam).
 - Students will recognize digital propaganda of websites and email

Cyber Ethics

Standard 3: Students recognize the ethical and legal issues while accessing, creating, and using digital tools and resources in order to make informed decisions.

Indicators:

1. Respect the copyright and intellectual property rights of others.
 - Students will recognize that it is illegal to download media or copy resources outside the copyright guidelines of Fair Use
 - Students will understand the term “copyright” and apply it to their own interaction on the Internet..
2. Identify plagiarism when using digital tools and content.
 - Students will understand the term “plagiarism” and recognize that copying content directly from the Internet and claiming it as their own is stealing and against the law.
 - Students will identify hacking and recognize the legal ramifications.
 - Students will only use their personal login and password
 - Students will understand that unauthorized access to computer programs and systems carries legal consequences. Understand the legal, ethical, and privacy guidelines for emailing and viewing/posting content.
3. Students will recognize that posting inappropriate pictures of themselves and others is wrong.
 - Students will only use their personal login and password.
 - Students will understand that unauthorized access to computer programs

- and systems carries legal consequences.
4. Students will recognize that sending inappropriate emails about others is wrong.
 - Students will recognize that posting inappropriate pictures of themselves and others is wrong.
 - Students will recognize that sending inappropriate emails about others is wrong.
 - Students will understand that posting or commenting on anything that could hurt others is wrong.
 - Students will understand when it is appropriate to forward digital communication (e.g., email, text messages, pictures, videos).
 5. Recognize the responsibility, legal consequences, and emotional effects of cyberbullying.
 - Students will recognize that bullying online is the same as real life bullying.
 - Students will refrain from repetitive, unwanted digital communication.

Personal Safety

Standard 4: Students will recognize online risks and dangers in order to take appropriate actions to protect themselves while using digital tools and resources.

Indicators:

1. Recognize attempts at phishing for information.
 - Students will understand the term “phishing” and be taught not to open up email messages from people they do not recognize.
 - Students will understand the consequences of responding to or forwarding phishing scams.
2. Implement procedures to protect computer systems from viruses and hackers.
 - Students will understand what an email attachment is and what it can do.
 - Students will distinguish between appropriate and inappropriate email attachments.
 - Students should not open questionable email attachments without asking an adult
3. Recognize the tactics that online predators use to lure students.
 - Students will not talk to strangers online.
 - Students will tell an adult if someone online makes them feel uncomfortable.
 - Students will not give out any personal information (e.g., name, address, phone number, email address, school name, personal description).
 - Students will recognize that an adult predator may pose as a child online.

4. Avoid access to controversial content.
 - Students will only go to sites that have been approved by an adult or use a child-friendly search engine.
 - Students should not sign up for an account on any website without adult approval.
5. Avoid sharing personal logins and passwords.

Students will never tell anyone their personal login or password.
6. Identify the type of information that may lead to identity theft.

Students will not give out any personal information (e.g., name, address, phone number, email address, school name, personal description).
7. Identify the appropriate use and safety precautions when participating in online activities.
 - Students will not give out personal information online.
 - Students should only participate in chatrooms, instant messaging, social networking, and online games with the permission and supervision of an adult.

Middle Grades (Grades 6-8)

Digital Citizenship

Standard 1: Students recognize their rights and responsibilities in using technologies within the context of today's world.

Indicators:

1. Recognize that content uploaded to the web is accessible to everyone and creates a reflection of who you are throughout your life.
 - Students will use discernment when posting content on email, websites, social networks, wikis, blogs and other collaboration tools.
 - Students will understand that internet content can be archived and can exist forever.
 - Students will understand that digital content sent via phone, cameras, and other digital devices can be archived and can exist forever.
2. Understand the difference between reality and virtual citizenship as it pertains to virtual games and virtual worlds.
 - Students will understand the difference between interacting in a virtual world and the real world.
 - Students will understand the responsibility of virtual citizenship.
 - Students will recognize the risks and symptoms of online addiction.
3. Exhibit responsibility, safety and etiquette when communicating digitally.
 - Students will safely and responsibly use various forms of communication.
 - Students will recognize who has access to view and respond to communication.
 - Students will understand that online communication, including email and text messaging, is never private and may be shared with others without your knowledge.
 - Students will communicate politely in email, wikis, blogs, and forums.
 - Students should communicate only in child-safe environments (e.g., epals, echalk, sharpschools, class blogmeister).
 - Students will understand that commercial email accounts outside the child-safe environment are exposed to risks.

Media Literacy

Standard 2: Students use critical thinking and evaluation while incorporating appropriate digital tools and resources into their education.

Indicators:

1. Recognize author bias, critically evaluate resources, and apply effective search practices when researching on the Internet.
 - Students will learn to identify the source of Internet content.
 - Students will learn to identify different domain types and their purpose (e.g., .org, .gov, .edu, .net, .com)
 - Students will learn to critically evaluate digital information.
 - Students will use teacher approved sites or approved search engines in a monitored environment.
 - Students will learn how to effectively use search strategies.
2. Collaborate safely, responsibly, and effectively when using wikis, blogs, email, and emerging technologies.
 - Students should use collaboration tools (e.g., Blackboard, Google Docs, wikis, blogs) only with adult supervision.
 - Students will learn to use appropriate collaboration tools and exhibit responsible behavior.
 - Students will learn how to interact appropriately (e.g., inflammatory language) on collaboration tools.
3. Understand the appropriate time and place to use instant messaging lingo and emoticons as they apply to formal and informal writing.
 - Students will understand that instant messaging lingo is a part of informal writing but not appropriate for all informal writing.
 - Students will understand when it is appropriate to use the conventions of written Standard American English in collaboration tools.
 - Identify digital propaganda (e.g., pop up ads, spam, advertisements)
 - Students will recognize the purpose of digital propaganda in websites and email.
4. Identify digital propaganda (e.g., pop up ads, spam).

Students will recognize the purpose of digital propaganda in websites and email.

Cyber Ethics

Standard 3: Students recognize the ethical and legal issues while accessing, creating, and using digital tools and resources in order to make informed decisions.

Indicators:

1. Respect the copyright and intellectual property rights of others.
 - Students will recognize that it is illegal to download media or copy resources outside the copyright guidelines of Fair Use
 - Students will understand the term “copyright” and apply it to their own interaction on the Internet.
 - Students will understand Fair Use and their obligations regarding citations and references.
2. Identify plagiarism when using digital tools and content.
 - Students will understand the term “plagiarism” and recognize that copying content directly from the Internet and claiming it as their own is stealing and against the law.
 - Students will understand their obligations regarding citations and references.
3. Identify hacking and recognize the legal ramifications.
 - STUDENTS WILL ONLY USE THEIR PERSONAL LOGIN AND PASSWORD.
 - Students will understand that unauthorized access to computer programs and systems carries legal consequences.
4. Understand the legal, ethical, and privacy guidelines for emailing and viewing/posting content.
 - Students will recognize that posting inappropriate pictures of themselves and others is wrong and can carry legal consequences.
 - Students will recognize that sending inappropriate emails about others is wrong and can carry legal consequences.
 - Students will understand that posting or commenting on anything that could hurt others is wrong and can carry legal consequences.
 - Students will understand when it is appropriate to forward digital communication (e.g., email, text messages, pictures, videos)
5. Recognize the responsibility, legal consequences, and emotional effects of cyberbullying.
 - Students will recognize that bullying online is the same as real life bullying and can carry legal consequences.
 - Students will refrain from repetitive, unwanted digital communication which can carry legal consequences.

Personal Safety

Standard 4: Students will recognize online risks and dangers in order to take appropriate actions to protect themselves while using digital tools and resources.

Indicators:

1. Recognize attempts at phishing for information.
 - Students will understand the term “phishing” and know when to open email messages from people they do not recognize.
 - Students will understand the consequences of responding to or forwarding phishing scams.
2. Implement procedures to protect computer systems from viruses and hackers.
 - Students will understand what an email attachment is and what it can do.
 - Students will distinguish between appropriate and inappropriate email attachments.
 - Students should not open questionable email attachments without asking an adult.
 - Students will learn to recognize file extensions such as .jpg, .exe, .doc
 - Students will learn to use software applications that will protect computer systems from viruses and hackers.
3. Recognize the tactics that online predators use to lure students.
 - Students will use caution when chatting online.
 - Students will not meet someone encountered online.
 - Students will tell an adult if someone online makes them feel uncomfortable or asks to meet them.
 - Students will not give out any personal information (e.g., name, address, phone number, email address, school name, personal description, photos, clubs).
 - Students will recognize that an adult predator may pose as a child online.
4. Avoid access to controversial content.
 - Students will only go to sites or search engines that have been approved by an adult in a monitored environment.
 - Students should not sign up for an account on any website without adult approval.
5. Avoid sharing personal logins and passwords.
 - Students will never tell anyone their personal login or password.
 - Students will understand the importance of logging out.
 - Students will understand the dangers of automatically saving logins and passwords on digital applications and web sites.

6. Identify the type of information that may lead to identity theft.

Students will not give out any personal information (e.g., name, address, phone number, email address, school name, personal description, social security number, school ID number).

7. Identify the appropriate use and safety precautions when participating in online activities.

- Students will not give out personal information online.
- Students should only participate in chatrooms, instant messaging, social networking, and online games with the permission and supervision of an adult.

High School (Grades 9-12)

Digital Citizenship

Standard 1: Students recognize their rights and responsibilities in using technologies within the context of today's world.

Indicators:

1. Recognize that content uploaded to the web is accessible to everyone and creates a reflection of who you are throughout your life.
 - Students will use discernment when posting content on email, websites, social networks, wikis, blogs and other collaboration tools.
 - Students will understand that digital content can affect college admissions and employment.
 - Students will understand that internet content can be archived and can exist forever.
 - Students will understand that digital content sent via phone, cameras, and other digital devices can be archived and can exist forever.
2. Understand the difference between reality and virtual citizenship as it pertains to virtual games and virtual worlds.
 - Students will understand the difference between interacting in a virtual world and the real world.
 - Students will understand the responsibility of virtual citizenship.
 - Students will recognize the risks and symptoms of online addiction.
 - Students will distinguish between real-world digital interaction and virtual interaction.
3. Exhibit responsibility, safety and etiquette when communicating digitally.
 - Students will safely and responsibly use various forms of communication.
 - Students will recognize who has access to view and respond to communication.
 - Students will understand that online communication, including email and text messaging, is never private and may be shared with others without your knowledge.
 - Students will understand that legal consequences are more serious once the age of majority is attained. (prosecution and inclusion on the sexual predator list are possible consequences of taking or sharing inappropriate pictures and videos.)

- Students will communicate politely in email, wikis, blogs, and forums.
- Students will understand that commercial email accounts are exposed to risks.

Media Literacy

Standard 2: Students use critical thinking and evaluation while incorporating appropriate digital tools and resources into their education.

Indicators:

1. Recognize author bias, critically evaluate resources, and apply effective search practices when researching on the Internet.
 - Students will learn to identify the source of Internet content.
 - Students will learn to identify different domain types and their purpose (e.g., .org, .gov, .edu, .net, .com)
 - Students will learn to critically evaluate digital information.
 - Students will use appropriate web sites and approved search engines in a monitored environment.
 - Students will learn to effectively use advanced search strategies.
2. Collaborate safely, responsibly, and effectively when using wikis, blogs, email, and emerging technologies.
 - Students should use appropriate collaboration tools (e.g., Blackboard, Google Docs, wikis, blogs) and exhibit responsible behavior.
 - Students will interact appropriately (e.g., inflammatory language) on collaboration tools.
3. Understand the appropriate time and place to use instant messaging lingo and emoticons as they apply to formal and informal writing.
 - Students will understand that instant messaging lingo is a part of informal writing but not appropriate for all informal writing.
 - Students will understand when it is appropriate to use the conventions of written Standard American English in collaboration tools.
4. Identify digital propaganda (e.g., pop up ads, spam).

Students will recognize the purpose of digital propaganda in websites and email.

Cyber Ethics

Standard 3: Students recognize the ethical and legal issues while accessing, creating, and using digital tools and resources in order to make informed decisions.

Indicators:

1. Respect the copyright and intellectual property rights of others.
 - Students will recognize that it is illegal to download media or copy resources outside the copyright guidelines of Fair Use
 - Students will understand the term “copyright” and apply it to their own interaction on the Internet.
 - Students will understand Fair Use and their obligations regarding citations and references.
2. Identify plagiarism when using digital tools and content.
 - Students will understand the term “plagiarism” and recognize that copying content directly from the Internet and claiming it as their own is stealing and against the law.
 - Students will understand obligations regarding citations and references.
3. Identify hacking and recognize the legal ramifications.
 - Students will only use their personal login and password.
 - Students will understand that unauthorized access to computer programs and systems carries legal consequences.
4. Understand the legal, ethical, and privacy guidelines for emailing and viewing/posting content.
 - Students will recognize that posting inappropriate pictures of themselves and others is wrong and can carry legal consequences.
 - Students will recognize that sending inappropriate emails about others is wrong and can carry legal consequences.
 - Students will understand that posting or commenting on anything that could hurt others is wrong and can carry legal consequences.
 - Students will understand when it is appropriate to forward digital communication (e.g., email, text messages, pictures, videos).
 - Students will understand that significant legal consequences are possible depending on student age and the offense.
5. Recognize the responsibility, legal consequences, and emotional effects of cyberbullying.
 - Students will recognize that bullying online is the same as real life bullying and can carry significant legal consequences depending on student age and the offense.
 - Students will refrain from repetitive, unwanted digital communication which can carry legal consequences.

Personal Safety

Standard 4: Students will recognize online risks and dangers in order to take appropriate actions to protect themselves while using digital tools and resources.

Indicators:

1. Recognize attempts at phishing for information.
 - Students will understand the term “phishing” and know when to open email messages from people they do not recognize.
 - Students will understand the consequences of responding to, forwarding, or participating in phishing scams.
2. Implement procedures to protect computer systems from viruses and hackers.
 - Students understand what an email attachment is and what it can do.
 - Students will distinguish between appropriate and inappropriate email attachments.
 - Students should understand the danger of opening questionable email attachments.
 - Students should understand the function of file extensions such as .jpg, .exe, .doc.
 - Students use software applications that will protect computer systems from viruses and hackers.
3. Recognize the tactics that online predators use to lure students.
 - Students will use caution when chatting online.
 - Students will not meet someone encountered online.
 - Students will tell an adult if someone online makes them feel uncomfortable or asks to meet them.
 - Students will not give out any personal information (e.g., name, address, phone number, email address, school name, personal description, photos, clubs, driver’s license, social security number, school ID number).
 - Students will recognize that an adult predator may be deceptive about their age, gender, or other characteristics.
4. Avoid access to controversial content.
 - Students will only go to appropriate sites or search engines.
 - Students should be aware that access to any website can be tracked and may have significant legal consequences.
5. Avoid sharing personal logins and passwords.
 - Students will never tell anyone their personal login or password.
 - Students will understand the importance of logging out.
 - Students will understand the dangers of automatically saving logins and passwords on digital applications and web sites.

6. Identify the type of information that may lead to identity theft.
 - Students will not give out any personal information (name, address, phone number, email address, school name, personal description, social security number, driver's license number, school ID number, etc.).
 - Students will understand the importance of preventing identity theft.
7. Identify the appropriate use and safety precautions when participating in online activities.
 - Students will not give out personal information online.
 - Students should use caution if participating in chatrooms, instant messaging, social networking, or online games.
 - Students should understand the dangers of using digital tools while driving (e.g., texting, cell phone use).

APPENDIX D - REFRESH RATE FOR DISTRICT OFFICE

School personnel refresh is included in the plan

<u>Position</u>	<u>Purchase date</u>	<u>Refresh date</u>
Custodian (OptiPlex 745)	June 2010	2017
Executive Secretary of Human Resources (OptiPlex 380)	September 2010	2017
Accounts Payable Clerk (Inspiron One 2020)	February 2013	2017
Payroll Specialist (Inspiron One 2020)	February 2013	2017
Purchasing Clerk (Inspiron One 2020)	February 2013	2017
Medicaid Clerk (Inspiron One 2330)	March 2013	2017
Receptionist (Dell Inspiron One 2020)	April 2013	2017
Director of Technology	June 2013	2017
Executive Secretary of Teaching and Learning (OptiPlex 9010)	September 2013	2017
Assistant Superintendent of Teaching and Learning (Asus)	January 2014	2018
Data Specialist (Asus)	January 2014	2018
Assistant Superintendent of Operations and Planning (April)	April 2014	2018
Food Service Director (Acer)	April 2014	2018
Food Service-Bookkeeper (Acer)	April 2014	2018
Chief Academic Officer (Thinkpad X240)	July 2014	2018
Superintendent	July 2014	2018
Assistant Superintendent of Human Resources (Latitude E7250/7250)	June 2015	2019
Digital Learning Coordinator (Latitude 3450)	August 2015	2019
Lead Nurse (OptiPlex 9010)	August 2015	2019
Benefits Coordinator (OptiPlex 380)	September 2015	2019
Computer Technician	September 2015	2019
Computer Technician	September 2015	2019
Computer Technician	September 2015	2019
Computer Technician	September 2015	2019
Executive Secretary of Operations and Planning	September 2015	2019
Help Desk Monitor (OptiPlex 3020M)	September 2015	2019
Maintenance Supervisor (Asus)	September 2015	2019
Transportation Assistant	September 2015	2019
Transportation Supervisor	September 2015	2019

Director of Finance (Latitude E7250) laptop	July 2016	2020
Director of Exceptional Services	April 2017	2021
Executive Secretary for the Superintendent	April 2017	2021
Parenting Coordinator	April 2017	2021
School Phycologist II	April 2017	2021
Special Services Speech Pathologist	April 2017	2021
School Phycologist II	April 2107	2021
Secretary of Exceptional Education	April 2107	2021
Special Services Clerk	April 2107	2021
Special Services Speech Pathologist	April 2107	2021

WORK IN PROGRESS

APPENDIX E

Chromebook Protection - Terms & Conditions 2016-2017

A prepaid Usage Fee of \$20 is required for all high school students before receiving their Chromebook. This amount covers accidental damage, reconfiguration, minor repairs and replacement Chromebooks.

The Chromebook being issued is ruggedized and meets military specs however, it is highly recommended that students procure a neoprene sleeve or protective case for their Chromebook. Sleeves are approximately \$10 and hard cases are approximately \$20.

The Usage Fee will NOT cover repairs resulting from the following:

- Broken screen (the \$20 Usage Fee will be deducted from actual cost of the screen however subsequent broken screens will be charged at full cost)
- Damage caused by abuse, misuse, flood, fire, earthquake, or other external cause
- Damage/Overheating as a result of being left in the sun, car, etc
- Damage as a result of a pet
- Damage from food, drink or other liquid
- Negligence (i.e. placement/storage in an unsafe location or position as to cause dropping)
- Damage caused by service performed by anyone who is not a representative of OCSD4
- Removal of the serial number
- Loaning your Chromebook or charger to another person
- Leaving the Chromebook or charger unattended will void the Usage fee and the student will be responsible for paying for a replacement
- Damage resulting from removal of any component of the Chromebook

Costs associated with the damages listed above will be assessed as follows:

<u>Component</u>	<u>Cost</u>
Chromebook (damaged beyond repair)	\$ 205
Screen assembly	\$ 100
LCD (screen) only	\$ 60
Plastic housing	\$ 30
Keyboard/Touchpad	\$ 70
Motherboard	\$ 85
Charging port	\$ 10
Charger	\$ 25

REFERENCES

- French, V. W. (1997). Teachers Must Be Learners, Too: Professional Development and National Teaching Standards. *NASSP Bulletin*, 81(585), 38-44. doi:10.1177/019263659708158507
- Joyce, B. & Showers, B. (2002). Student achievement through staff development. Alexandria, VA: Association for Supervision and Curriculum Development.
- Monahan, Jennifer (July 31, 2016). Technology in the 21st Century Classroom. *NHM (North Hills Magazine)*
- Theadaptiveteacher (October 6, 2016). Technology in the classroom: The SAMR model
- American School & University, Jan/Feb 2017, Kennedy, Mike Connecting to Things pg 16-20
- SC State Educational Technology Plan (2014-2016)
- The Horizon Report - 2016 K12 Edition
- Maryland Technology Literacy Standards
- ISTE Standards
- 2Revolutions Technology Combinations for Competency-Based Education
- National Education Technology Plan 2016 (US Department of Education)