

**Network Plan**

MEDT 7471

Spring 2011

Dr. Bray

University of West Georgia

Richard White

## Table of Contents

<b>1) Introduction to Our School</b>	<b>page 1</b>
<b>2) Hardware and Software Standards</b>	<b>page 4</b>
<b>3) Network Outline</b>	<b>page 10</b>
<b>4) Purchasing Policy</b>	<b>page 12</b>
<b>5) Security and Accessibility Plan</b>	<b>page 16</b>
<b>6) Acceptable Use Policy</b>	<b>page 19</b>
<b>7) Disaster Recovery</b>	<b>page 32</b>
<b>8) Disposal/Repurposing Policy</b>	<b>page 39</b>
<b>9) Professional Development</b>	<b>page 41</b>

## **Introduction to Our School**

This document serves as the guide for network services to be provided by the Board of Trustees to the Tech Prep Academy. Hereafter referred to as the Academy, this school is being designed to highlight what should be offered to students in the realm of in class technology at every school in the country. Although fictional and designed to meet the requirements of the MEDT 7471 course at the University of West Georgia, I feel that this school could and probably does exist somewhere in the world, even in the state of Georgia. Our school is a middle school and serves grades six through eight, we currently enroll approximately 1000 students and are a charter school receiving both public and private funding. We will be borrowing a great deal of our policy from the Cobb County School District and using The School Network Handbook as a guide for drafting this plan. I have also borrowed elements from the Denver Unified School District and Leon County Florida School District where needed. Cisco Systems provided a great deal of information for setting up a strong and forward thinking network.

Our school is ethnically diverse with a student population that is made up of approximately 42% white students, 36% African-American students, 20% Hispanic students, and the remaining 2% representing other ethnicities including Native American, Middle Eastern, and North African to name a few. Our student body is approximately 68% female and 32% male. Although we are in a middle to upper middle class area, many of our students live in the outlying areas and approximately 68% of them receive free or reduced lunches. This qualifies us for Title 1 funding and allows us to offer support and programming not typically found in public institutions. Within our students we serve approximately 10% in our special education services, 1% in our mildly or intellectually disabled services, and 1% in our deaf and hard of hearing services. These students are served through small group classes, mainstream and inclusion classes, self-contained small group classes, and mainstream or inclusion classes with interpreters.

We also serve approximately 2% of our students through our English speakers of other languages (ESOL) program where students are allowed to learn English and to learn in their native language. Finally we serve approximately 27% of our students through our gifted and creative education program, where they are allowed to partake in service learning and technology enhanced programming to prepare them for life after middle and high school.

Our staff is also very diverse and representative of our student and community populations. The staff is roughly 45% male and 55% female and it is culturally and ethnically diverse. Its make up reflects the make-up of the community and the school as a whole. This helps our students feel comfortable with their teachers, and makes transition from elementary to middle school a lot easier. Within our staff over 80% of them have advanced degrees and 70% of those have post-graduate degrees. We currently employ 100 general education teachers with credentials to match the needs of the school, every teacher is dual certified to maximize their use and subject knowledge. We strive to keep class sizes between 10 and 12 students and allow no more than 15 per class. The school also employs 6 deaf and hard of hearing teachers, 15 special education teachers, 6 mildly or intellectually disabled teachers, 15 general education paraprofessionals, 4 administrators, 3 office support staff members, 2 media specialist, 1 media paraprofessional, 3 counselors, 6 deaf and hard of hearing interpreters, 2 ESOL translators/parent facilitators, and 1 book keeper with grant writing experience. This allows us to give our students the personal attention and help they need and deserve.

Our classrooms are set up to encourage social and problem based learning experiences. Every students is given an opportunity to take courses in physical education, art, music, foreign languages, technology, and science exploration to name a few. The school also offers an extensive club selection as well as a news team and yearbook experience. We also publish a

school newspaper through our journalism connections course once per week. The teachers have two hours of planning time and offer extensive help after school hours and before school hours to accommodate parent and student availability and scheduling. We meet with parents twice per year and make every teacher available for by appointment meeting times.

## Hardware and Software Standards

### **Administrative Technology Standards**

**Administrative Software** – DOTS refers to the department of technology services. All software is recommended at current release version. Adobe products will be included in rollout of district wide use of Adobe Creative Suite 5 or 6.

	User License Req?	District License	Minimum Version Standard	Recommended Version Standard
<b>Desktop Applications</b>				
Adobe Acrobat Reader	N	N	7.0	X
Adobe Acrobat Writer	Y	N	7.0	X
Internet Explorer	N	NA	7.0 SP1(PC) Not supported (Mac)	9.0 (PC) Not supported (Mac)
Firefox	N	NA	2.0.0.20 (Mac 10.3.9) 3.6 (Mac 10.4.11, 10.5.8, 10.6.3)	2.4 (Mac 10.3.9) 3.6 (Mac 10.4.11, 10.5.8, 10.6.3) 3.6 (PC)
Java	N	NA	1.4	Current
Mac OS	N**	NA	10.3.9, 10.4	10.5 (PPC) 10.6

				(Intel)
McAfee Virus Scan	N	Y	MAC – Virex 7.7 PC – 8.5  (all PCs should be automatically updated by EPO)	MAC – Current PC –Current
MS Office Professional - Word, Excel, Access, PowerPoint, Outlook	N	Y	MAC – MS Office 2004  PC – MS Office 2003	MAC – MS Office 2008  PC – MS Office 2010 Pro
MS Project	Y	N	PC – MS Project 2003	PC – MS Project 2010
MS Visio	Y	N	PC - MS Visio 2003	PC - MS Visio 2010
Windows OS	N	Y	Windows XP, Vista, 7	Windows 7

\*\*Anything greater than OS 10.3.9 requires a user license

### **Administrative Hardware Standards for the 2010-2011 School Year**

Hardware	Minimum Version Standard	Recommended Version Standard
<b>Computers</b>	1 GB of RAM. 80 GB hard drive. CD optical drive. Laptops must have wireless support for 802.11g, WPA with TKIP, 802.1X using PEAP to connect to DPS wireless networks.	4 GB of RAM, 1 TB hard drive. DVD+/-RW. 256 MB video card.

Dell		Manufacturer's recommended model. For further information, visit Dell's premier web page. You may link to that web page from:  <a href="http://luxo.dpsk12.org/calculator/">http://luxo.dpsk12.org/calculator/</a>
Macintosh		Manufacturer's recommended model. For further information, visit the Apple Store web page. You may link to that web page from:  <a href="http://luxo.dpsk12.org/calculator/">http://luxo.dpsk12.org/calculator/</a>
NComputing	NComputing may be used to share a single Windows processor to several workstations. Please consult with DoTS for limitations.	
<b>Network Cards for Printers</b>		
Hewlett Packard	Manufacturer's recommended model	Manufacturer's recommended model
<b>Printers</b>		
Hewlett Packard	HP LaserJet or Color LaserJet  <a href="http://luxo.dpsk12.org/calculator/">http://luxo.dpsk12.org/calculator/</a>	HP LaserJet or Color LaserJet  <a href="http://luxo.dpsk12.org/calculator/">http://luxo.dpsk12.org/calculator/</a>

### Programming and System Development Software

	User License Required?	District License	Minimum	Version Standard	Recommended Version Standard
Visual Studio	Y	N	2008	2010	No

\* Support from the Department of Technology Services will be dependent on available resources and project priorities.

### Enterprise Server Operating System



	<b>User License Required?</b>	<b>District License</b>	<b>Minimum</b>	<b>Version Standard</b>	<b>Recommended Version Standard</b>
MS Windows	N	N	Windows 2008	Windows Current	Yes

#### Enterprise Relational Database Management Software

	<b>User License Required?</b>	<b>District License</b>	<b>Minimum</b>	<b>Version Standard</b>	<b>Recommended Version Standard</b>
MS SQL Server	N	N	2005 SP3	Current	No
Oracle *	N	Y	8.1.7	11G Release 1	No

\* Oracle is currently supported for existing applications, but no new Oracle databases will be implemented

#### Application Server Software

	<b>User License Required?</b>	<b>District License</b>	<b>Minimum</b>	<b>Version Standard</b>	<b>Recommended Version Standard</b>
Microsoft IIS *	N	Y	Version 6	Version Current	No
Microsoft SharePoint	N	Y	2007	Current	No
Microsoft .NET	N	Y	2.0	Current	No

\* Primary Implementation – Multiple sites per machine, served and possibly load balanced via Microsoft ISA

#### Storage

Storage Area Network via Fiber Channel (EMC Storage, Cisco MDS and Emulex Host Cards)  
Local storage for Enterprise Source data is highly discouraged

#### Enterprise Directory Services

DPS has a fully functional Microsoft Active Directory 2008 (AD) implementation. Applications and systems should be developed and implemented to either use AD directly or via the LDAP3 and above standard for Authentication and Application Security.

## **Virtualization**

Microsoft Hyper-V is the District's Virtualization platform and the use of this technology is strongly recommended. This is one of the major technology and green initiatives for DPS. Systems that require physical servers are highly discouraged.

## **Additional Information**

### **Software Installation**

- Certain software packages will not co-exist on certain workstations.
- Hardware is expected to meet the recommended district standard before installing any software (including the operating system).
- For recommendations on educational software contact your school's Educational Technology representative.

### **Back Ups**

- DoTS is responsible for backing up the district servers on a regular basis.
- Backup of servers at schools is the responsibility of the school.
- End users are responsible for backing up their files – DoTS recommends backups be done on electronic media, such as a CD-R or a tape backup.

### **Hardware Setup**

- An onsite visit from DoTS is required before purchasing new networking equipment.
- File transfers are the ultimate responsibility of the end users.
- New Internet connections must be Ethernet-connected.
- Peripherals (network cards, scanners, etc.) are recommended on an individual basis.
- For recommendations on server configuration contact the DoTS Hotline.

### **Support**

- Sites will be given information on outsourcing technical support if the requests or problems go beyond DoTS expertise or if the request cannot be accomplished in the available time frame.
- Donated equipment that was received following district procedures will be supported but functionality cannot be guaranteed.
- DoTS reserves the right to remove unauthorized hardware and software from the DPS network.

### **Databases and Reporting Tools**

- DoTS supports the functionality of standardized databases and reporting software designed by DoTS and located on a server hosted on-site at DoTS
- Legacy multi-user databases that contain a current migration plan will be supported.

### **Telecommunications**

- For recommendations regarding voice, video, or data wiring, contact the DoTS Hotline

### **Rollout of Future Releases of Software**

- New releases of desktop application software are evaluated by DoTS and upon approval will be included in district standards.

**Hardware repair is the responsibility of schools and departments for equipment no longer under warranty.**

## **Network**

The most important part of the school network is the backbone upon which all services will operate. Without a solid backbone services will be slow, and interruptions will be persistent. In order to support the forward thinking and additional services required by today's technology driven classrooms, we will wire our school with a 100% fiber optic backbone. This will provide us with connectivity at the maximum speeds possible. This fiber optic backbone will be backed up by a parallel twisted pair copper backbone capable of Gigabit Ethernet speeds. This will ensure that multimedia streaming and video conferencing occurs with little lag time and data movement is quick and secure. Connections to the network will be made through 1000Base-T connections and at a minimum 100Base-T connections using twisted core copper wiring.

Our 55 classrooms, offices, and other areas will be connected to the network using Cisco Systems routers, switches, boosters, and wireless networking tools. Please see the diagram below for the specific items to be used according to Cisco Systems recommendations. Specific numbers of products will be based on final needs of the system, but will be duplicated to insure constant connection to the main server and to online services. Wireless access is included in this system. All data will be backed up by servers onsite and by a cloud service to be subscribed to later. There will also be data backup, hard wired offsite to insure that we have retrievable access to school and student data if there is a major catastrophe. This system will be Windows based, but will allow full access by Mac and Linux machines.

This document, contains the network diagram, and a list of all the platforms and software releases which were validated for the Schools Service Ready Architecture (SRA). The last section includes the configurations for each platform (CLI only, no GUI).

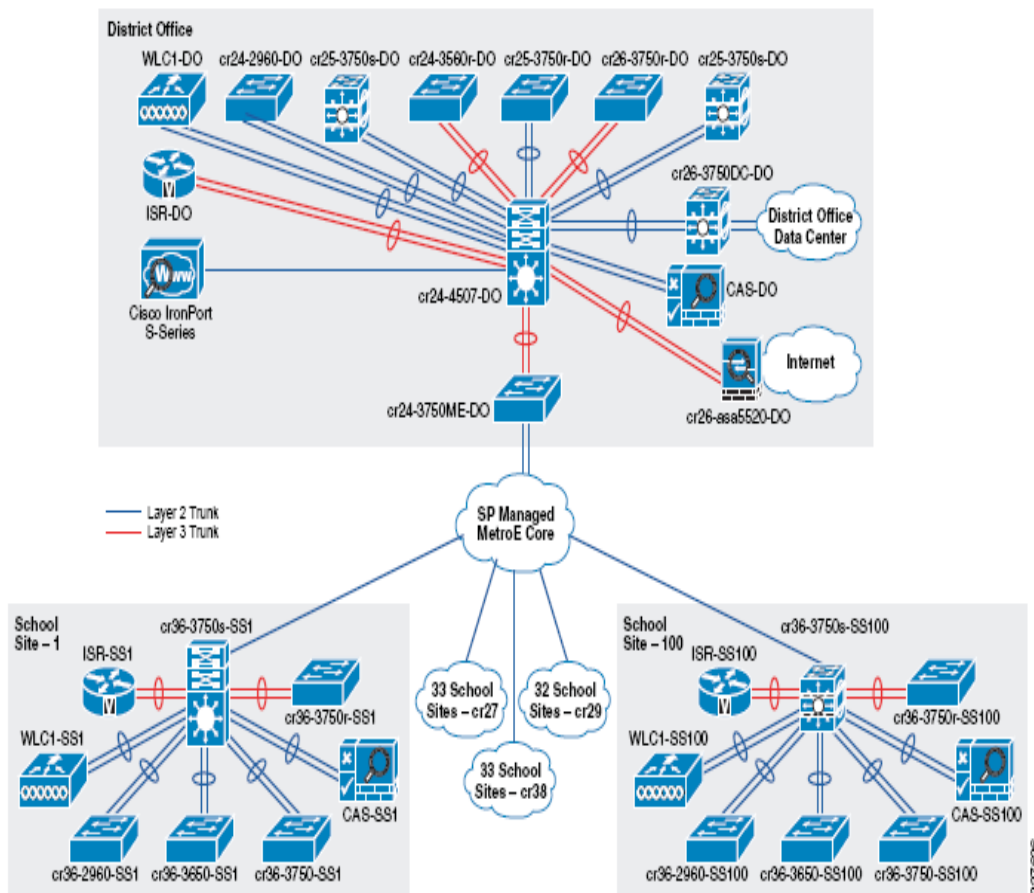
Provides a efficient and flexible network architecture for secondary schools, while enabling advanced services, such as security, unified wireless access, unified voice communications services, and presence services. The network is designed to meet the needs of the education environment:

- Academic Excellence
- Administrative Efficiency
- School safety and security

### Network Diagram

Figure 1 shows the network diagram for the School SRA.

Figure 1 Physical Topology



## **Hardware and Software Purchasing and Installation**

(1) The Purchasing Section is committed to the active pursuit and solicitation of maximum vendor response and participation in the acquisition of materials, supplies and services on behalf of the Academy. The essence of this statement of purchasing policy is to foster a structured system of open competition which will enable the District to purchase needed materials, supplies and services of the appropriate levels of quality at the lowest possible cost.

(2) When all other factors are equivalent, it is the intent of the Academy to acquire its goods and services from local vendors; however, the overall objective of acquiring the required product at the lowest possible cost will not be compromised in favor of supporting local vendors.

(3) The Purchasing Director shall, under the direction of the Superintendent, advertise and secure formal competitive bids, as provided in the applicable statutes and State Board of Education Administrative Regulations, for materials, supplies or services whose total cost is more than twenty-five thousand dollars (\$25,000). These bids shall be presented to the School Board for approval before any funds are encumbered or expended. Exceptions to these requirements are items listed on established state contract and those items specifically exempted by State Board of Education Regulations.

The securing of formal competitive bids for items costing more than \$25,000 will be waived by the School Board upon recommendation by the Superintendent or his designee in cases of extreme emergency or when only a single or sole source bidder is available to meet the required specifications. An emergency purchase is one brought about by a sudden unexpected event or by circumstances or caused beyond the control of the Board. A single or sole source item is a commodity or service for which an individual, or group of individuals, has the sole and exclusive right to manufacture and/or sell or provide, or a commodity which must be compatible with existing district equipment or operation. Such waivers must be based upon conditions and criteria congruent with applicable State Statutes and Regulations. Those exceptions or waivers for items costing \$25,000 or less may be administered by the Purchasing Director by promulgating procedures which specify the conditions and circumstances under which such waivers would be consistent with the overall intent and substance of this purchasing policy.

(4) The authority to make purchases and to expend monies which are properly budgeted for materials, supplies, and services not on established state contract and not otherwise exempt from bidding by state law and/or State Board of Education Regulations, shall be vested in the Purchasing Director under the direction of the Superintendent for those materials, supplies and services whose total cost is not more than twenty-five thousand dollars (\$25,000), provided:

(a) The Purchasing Director has secured competitive written, sealed quotes for items or a group of like items whose total cost is more than fifteen thousand (\$15,000), but less than twenty-five thousand dollars (\$25,000). These bids do not require School Board approval.

(b) The Purchasing Director has secured informal competitive telephone quotes for items or a group of like items whose total cost is more than eight thousand dollars (\$8,000), but less than fifteen thousand dollars (\$15,000). These bids do not require School Board approval.

(5) The authority to make purchases and to expend monies which are properly budgeted for materials, supplies and services which are established state contracts, cooperative bid agreements which are awarded by other Georgia school boards, city or county governmental agencies, Georgia community colleges, or the State University System to be used for purchasing items at the contracted unit price when bids permit such purchases, or otherwise exempt by state law and/or State Board of Education Regulation, shall be vested in the Purchasing Director, under the direction of the Superintendent. Any purchases made under this authority are not subject to School Board approval.

(6) Purchases of perishable produce are exempt from formal bid procedures. The Director of Food Services, under the direction of the Superintendent and the Purchasing Director, has authority to accept informal quotes from available providers, make purchases, expend budgeted funds and accept perishable produce without School Board approval of the bid quotes.

(7) For purposes of quality control, guidelines for evaluating products obtained and for compiling information about purchases of substandard or unsatisfactory goods and services shall be established. Vendors who fail to provide satisfactory goods or services may be removed from the bidders' list by the Superintendent. Such vendors may also be returned to the bidders' list at the discretion of the Superintendent.

(9) Leases, Lease-Purchases and Installment Sales Contracts.

(a) The School Board shall approve, and the Board Chair shall sign, all lease and lease-purchase and installment sales contracts with private individuals, corporations, or governmental agencies for the acquisition of equipment and property items needed for educational purposes regardless of fund source. No lease, lease-purchase or installment sales contract shall be entered into without specific Board approval prior to issuance of a purchase order even if the item is a sole source item or is on state contract. No lease or lease-purchase agreement shall be entered into for items whose total cost is less than \$5,000.

(b) Lease, lease-purchase or installment sales contracts shall be for periods not to exceed three years with a specified yearly payment rate and interest rates not in excess of those authorized by law. All lease renewals must be approved by the School Board. Schools or divisions requesting lease, lease-purchase or installment sales contracts shall budget sufficient funds for the cost in the budget of each year of the contract and shall have the appropriate Area Director or Assistant Superintendent sign off prior to requesting School Board approval.

(1) Copiers -Rental leases only are allowable for copiers. Copiers shall not be purchased through a lease purchase agreement. Copier lease periods cannot exceed three (3) years. Copier equipment utilizing network capabilities is considered a computer equipment equivalent purchase and shall be subject to the same review process that is required for computer equipment.

(2) Software -Lease purchases of software cannot exceed three (3) years. Multi year lease purchases of educational software must be approved by Technology and Information Services

and the Division of Teaching and Learning to ensure the software is compatible with the Academy's Technology Plan and curriculum goals.

(3) Computer/Equipment Hardware -Capital leases for computer hardware cannot exceed three (3) years. The computer equipment being acquired must be approved by Technology and Information Services to ensure the hardware is in compliance with the Academy's Technology Plan.

(c) Refinancing of lease, lease-purchase agreements or installment sales contracts is permitted to take advantage of a lower interest rate than that of the initial transaction and shall be approved in advance by the Board.

(10) Change Orders. The Superintendent and/or his designated administrator shall have the authority to approve change orders to construction contracts, for products or services totaling \$25,000 or less, provided that funds for securing such products or services have been properly budgeted within the project budget and that the total amount of all change orders so approved does not exceed one percent (1%) of the total amount originally budgeted for the project. Any such action shall be brought to the School Board for ratification, at the Board's next regular meeting.

Change orders exceeding \$25,000 shall require Board approval initially. Other purchasing and capital outlay requirements which affect the proper processing of construction change orders are not affected by this provision.

(11) Consultant Agreements. The Superintendent, or the Superintendent's designee, shall have the authority to approve consultant agreements for products or services totaling \$25,000 or less, provided that funds for securing such products or services have been properly budgeted. Consultant agreements exceeding \$25,000 shall require Board approval unless exempt under State Board of Administration Rules. This section shall not apply to professional services rendered by any architect, professional engineer, landscape architect, or registered land surveyor.

(12) Acquisitions for Technology and Information Services.

(a) Purchases of computer hardware, software, digital copiers and technical services acquisitions must be in accordance with the Board-adopted Master Plan for Technology and Information Services. Additionally, all such purchases shall have the approval of the Georgia Department of Education when the dollar amount exceeds those limits established by State Board Rules and/or Legislative mandate.

(b) The Executive Director of Technology and Information Services must review and approve all purchases of computer hardware, software, digital copiers and technical services acquisitions exceeding \$750.00. That approval signifies agreement with the acquisition and that the objectives to be accomplished are in accord with the district's long-range plans and promulgated standards.



(13) All purchases made using the Academy Visa Card will be in accordance with all purchasing policies.

(14) An Leon Academy Purchasing Manual will be disseminated to all schools and departments, setting forth detailed procedures and practices for implementing the appropriate purchasing policies.

All expenditures of the Academy will be in accordance with this policy and the purchasing manual.

The Superintendent will update the purchasing manual as necessary to provide purchasing guidelines for changes imposed by the Academy, State Board of Education or by other legal requirements imposed by the Legislature.

## Security and Accessibility Policy

The Academy believes that technology and its utilization enhances the quality and delivery of education and is an important part of preparing children for life in the 21st century. The community of technology users must understand that the Internet is a global, fluid community, which remains largely unregulated. While it is an extremely valuable educational tool, there are sections that are not commensurate with community, school, or family standards. The District believes that the Internet's advantages far outweigh its disadvantages and will provide an Internet filtering device which blocks access to a large percentage of inappropriate sites. It should not be assumed that users are completely prevented from accessing inappropriate materials or from sending or receiving objectionable communications.

Additionally, the District considers access to the Internet and computer resources a privilege, not a right. Therefore, users violating the District's Administrative Rules may be subject to revocation of these privileges and potential disciplinary action.

### **RULE:**

#### **A. GENERAL PROVISIONS:**

##### **1. Children's Internet Protection Act of 2000 (CIPA):**

The District will have the following in continuous operation, with respect to any computers belonging to the District having access to the Internet:

a. A qualifying "technology protection measure," as that term is defined in CIPA; and

b. Procedures or guidelines developed by the Curriculum and Instruction Division and the Technology Services Division which provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are obscene, pornographic, or harmful to minors, as those terms are defined in CIPA. Such procedures or guidelines will be designed to:

- (1) Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the World Wide Web;
- (2) Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- (3) Prevent unauthorized access, including so-called “hacking,” and other unauthorized activities by minors online;
- (4) Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and
- (5) Restrict minors’ access to materials “harmful to minors,” as that term is defined in CIPA.

## **2. Safety Risks:**

Teachers and others working with students will endeavor to caution students that they should:

- a. Never place personal contact information or a personal photograph on the Internet, e-mail or any on-line communication device. Personal contact information includes full name, address, telephone number, school address, or names of family or friends.
- b. Never arrange a face-to-face meeting with someone you meet online.
- c. Never open attachments or files from unknown senders.
- d. Always report to a teacher any inappropriate sites you observe being accessed by another user or that you access accidentally.

## **3. Internet Searches:**

Students should be supervised by instructional personnel when accessing network and internet resources and the following guidelines apply:

- a. Elementary School:  
Elementary school students may visit sites a teacher has pre-selected for them. Searches should be completed with child friendly Internet search engines (for instance see: [www.nettrekker.com](http://www.nettrekker.com))
- b. Middle School/High School:  
Middle school and high school students may visit sites a teacher has pre-selected for them. They may use search engines other than child-friendly search engines when directed to do so by their teacher.
- c. Non-instructional personnel, such as After School Program (ASP) workers, are not permitted to allow students to access technology resources unless it is an instructional activity.

## **4. Network Security:**

Maintaining network security is the responsibility of all users. Users should:

- a. Not leave an unsecured workstation without logging out of the network;
- b. Not share or disclose passwords; and

c. Notify appropriate personnel immediately if a potential security problem is identified.

All employees and students will be allowed equal access to computer and data gathering technology as available. Specific policies regarding use will be found in the Academy's Acceptable Use Policy. The District will require user names and passwords to enter secured areas of the network, and will restrict most access to on campus or onsite use. Parents will have access to their student's records via an assigned user name and password accessible from anywhere.

## Acceptable Use Policy

The Academy believes that technology and its utilization enhances the quality and delivery of education and is an important part of preparing children for life in the 21st century. The community of technology users must understand that the Internet is a global, fluid community, which remains largely unregulated. While it is an extremely valuable educational tool, there are sections that are not commensurate with community, school, or family standards. The Academy believes that the Internet's advantages far outweigh its disadvantages and will provide an Internet filtering device which blocks access to a large percentage of inappropriate sites. It should not be assumed that users are completely prevented from accessing inappropriate materials or from sending or receiving objectionable communications. Additionally, the Academy considers access to the Internet and computer resources a privilege, not a right. Therefore, users violating the Academy's Administrative Rules may be subject to revocation of these privileges and potential disciplinary action.

### A. GENERAL PROVISIONS:

#### 1. Children's Internet Protection Act of 2000 (CIPA):

The Academy will have the following in continuous operation, with respect to any computers belonging to the Academy having access to the Internet:

- a. A qualifying "technology protection measure," as that term is defined in CIPA; and
- b. Procedures or guidelines developed by the Curriculum and Instruction Division and the Technology Services Division which provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are obscene, pornographic, or harmful to minors, as those terms are defined in CIPA. Such

procedures or guidelines will be designed to:

- (1) Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the World Wide Web;
- (2) Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- (3) Prevent unauthorized access, including so-called “hacking,” and other unauthorized activities by minors online;
- (4) Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and
- (5) Restrict minors’ access to materials “harmful to minors,” as that term is defined in CIPA.

## 2. Safety Risks:

Teachers and others working with students will endeavor to caution students that they should:

- a. Never place personal contact information or a personal photograph on the Internet, e-mail or any on-line communication device. Personal contact information includes full name, address, telephone number, school address, or names of family or friends.
- b. Never arrange a face-to-face meeting with someone you meet online.
- c. Never open attachments or files from unknown senders.
- d. Always report to a teacher any inappropriate sites you observe being accessed by another user or that you access accidentally.

### 3. Internet Searches:

Students should be supervised by instructional personnel when accessing network and internet resources and the following guidelines apply:

#### a. Elementary School:

Elementary school students may visit sites a teacher has pre-selected for them.

Searches should be completed with child friendly Internet search engines (for instance see: [www.nettrekker.com](http://www.nettrekker.com))

#### b. Middle School/High School:

Middle school and high school students may visit sites a teacher has pre-selected for them. They may use search engines other than child-friendly search engines when directed to do so by their teacher.

c. Non-instructional personnel, such as After School Program (ASP) workers, are not permitted to allow students to access technology resources unless it is an instructional activity.

### 4. Network Security:

Maintaining network security is the responsibility of all users. Users should:

a. Not leave an unsecured workstation without logging out of the network;

b. Not share or disclose passwords; and

c. Notify appropriate personnel immediately if a potential security problem is identified.

### 5. Acceptable Use Agreement:

Prior to receiving access to the District's technology resources, employees and students (Form A) should complete an Acceptable Use Agreement indicating

they accept and agree to the provisions of this rule.

6. Copyright:

a. Students and employees should comply with Academy Administrative Rule C-1 (Intellectual Property), as well as federal, state or local laws governing copyrighted material.

b. Students/employees will not:

(1) Download or upload files to the Academy's technology that might cause copyright infringement; or

(2) Install, use, store, distribute or transmit unauthorized copyrighted or trademarked materials on Academy technology.

7. If students or employees believe that the implementation of this Rule denies access to material that is not prohibited by this Rule, he/she should submit that concern in writing to the school principal or designee or his/her supervisor or designee. The principal, supervisor or designee should report this concern to the appropriate District office within ten (10) school days.

**B. AUTHORITY:**

1. The Academy:

The Academy provides its students and authorized employees with access to and use of its technology consistent with the Academy's vision and strategic goals. Therefore, the Academy reserves the right to monitor, access, and disclose the contents of any user's files, activities, or communications to any appropriate authority, including law enforcement.



## 2. Employees:

Principals and Administrators will endeavor to inform students and employees of the responsibilities associated with use of the Academy's technology. To this end, Rule this rule is included in the Parent Information Guide. Any attempts to harm, modify, destroy or otherwise change the Academy's data and technology should be reported to appropriate Academy authorities. Staff will refer to District Administrative Rules governing employee and student conduct, including, Rules C1-106 collectively known as the Student Conduct: Codes of Conduct, when addressing inappropriate use or abuse of Academy technology privileges.

## 3. Students:

Students will adhere to all policies, Rules and regulations issued by the District and the Academy.

## C. PROHIBITED USES:

Students and employees who violate District/Academy policies, Rules or regulations governing the use of the District's technology and network resources may have their network privileges suspended or revoked and will be subject to District Administrative Rules applying to employee and student conduct including, for students, the provisions of the appropriate District Code of Conduct. Ethical use of Academy technology prohibits the following activities by all users:

### 1. Accessing, sending, creating or posting material or communication that is:

- a. Damaging;
- b. Abusive;
- c. Obscene, lewd, profane, offensive, indecent, sexually explicit, or pornographic;

- d. Threatening or demeaning to another person; or
  - e. Contrary to the District's Rules on harassment and/or bullying.
2. Posting anonymous or forging electronic communications.
  3. Using the network for financial gain, advertising or political lobbying to include student elections.
  4. Engaging in any activity that wastes, monopolizes, or compromises the District/Academy's technology or other resources.
  5. Illegal activity, including but not limited to copying or downloading copyrighted software, music or images, or violations of copyright laws.
  6. Using the Academy network for downloading music or video files or any other files that are not for an educational purpose or, for students, a teacher-directed assignment.
  7. Attempting to gain unauthorized access to District/Academy technology resources whether on or off school property.
  8. Using non-educational Internet games, whether individual or multi-user.
  9. Participate in any on-line communication that is not for educational purposes or, for students, that are not specifically assigned by a teacher.
  10. Using voice over IP, internet telephony, video and/or audio communication devices without teacher supervision.
  11. Using District/Academy technology resources to gain unauthorized access to another computer system whether on or off school property (e.g. "hacking").
  12. Attempting to or disrupting District/Academy technology resources by destroying, altering, or otherwise modifying technology, including but not limited to, files, data, passwords, creating or spreading computer viruses, worms, or Trojan horses;

engaging in DOS attacks; or participating in other disruptive activities.

13. Bringing on premises any disk or storage device that contains a software application or utility that could be used to alter the configuration of the operating system or network equipment, scan or probe the network, or provide access to unauthorized areas or data.
14. Attempting/threatening to damage, destroy, vandalize, or steal private/school property while using school technology resources.
15. Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies.
16. Using or attempting to use the password or account of another person, utilizing a computer while logged on under another user's account, or any attempt to gain unauthorized access to accounts on the network.
17. Connecting to or installing any personal technology computing device or software without prior approval of the District's Technology Services Division.
18. Attempting to obtain access to restricted sites, servers, files, databases, etc.
19. Exploring the configuration of the computer operating system or network, running programs not on the menu, or attempting to do anything not specifically authorized by District personnel or policies, Rules or regulations.
20. Leaving an unsecured workstation without logging out of the network.

#### D. E-MAIL:

E-mail accounts are provided to employees for professional purposes (see Administrative Rule COM-1A [Communications System: District's Inter and Intra Communications]). Students may access their personal e-mail accounts for educational purposes. Where

used in the following guidelines, User/Users refers to both employees and students:

1. Persons outside the District may be able to receive information regarding an employee's communications and use of the network from the District. (See Administrative Rule EHB [Data/Records Retention]).
2. Employees should request permission from the appropriate administrator prior to sending an e-mail message to an entire school staff or District level division.
3. Employee use of e-mail to transmit confidential student information, as defined in Rule SR-1 (Student Records), or sensitive personnel information is prohibited, except where the confidential information is sent in an e-mail directly to a parent/guardian, the subject of the e-mail, or a school official.
4. When an employee sends e-mail that contains confidential information, the employee should refer to the subject of the e-mail by first name only and should include the following disclaimer:

"This e-mail may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any unauthorized dissemination, distribution or copying of any information from this e-mail is strictly prohibited. If you receive this e-mail in error, please notify us immediately by collect telephone call at (telephone number) or electronic mail (e-mail)."
5. The District reserves the right to monitor whatever a User does on the network and to make sure the network functions properly.
6. A User has no privacy as to his/her communications or the uses he/she makes of the Internet.

7. Users should not use e-mail for personal gain or personal business activities.
8. Users will not use e-mail to distribute inappropriate material through pictures, text, forwards, attachments, and other forms of information.
9. Users will not send anonymous e-mail, nor will they harass others through e-mail.

E. WEB SITE PUBLISHING:

1. Publication of student information, work and pictures is governed by Administrative Rule SRD-2 (Monitoring-Recording Staff and Students).
2. Web pages or blogs hosted on or linked from the county school district's web server will not:
  - a. Include any information that indicates the physical location of a student at a given time, other than attendance at a particular school or participation in school activities where appropriate consent has been received.
  - b. Display personal information, photographs, videos, streaming video, or audio clips of any identifiable student without a prior written permission slip (Form PDSP-SW (Permission to Display Student Photograph) if a parent/guardian has "opted out" of the release of directory information as stated in the Directory Information Statement in the Parent Information Guide.
3. Prior to placing a student's material on the Internet, the student should sign Form PDSP-SW (Permission to Display Student Work). For students under the age of 18, the permission slip should also be signed by the student's parent/guardian.
4. Students may retain the copyright on the material they create that is subsequently displayed or performed on the Academy's Web site or individual school Web pages or blogs.

## F. EMPLOYEE CREATED WEB PAGES AND/OR BLOGS:

The Academy assumes no responsibility for schools or individual employees who do not comply with the following provisions:

1. Employees may create or link to individual Web pages and/or blogs on an external site provided these external sites meet the Academy's definition of "educational purposes" as stated in Section G below. Any links to external sites that fail to meet that definition will be removed.
2. Each employee will be responsible for maintaining his/her Web pages or blogs in cooperation with the school Web Publisher. Specifically, all material originating from the employee and placed on the employee Web pages/blogs will be consistent with the Web Page Publishing and Compliance Guidelines (Form WPPCG) and approved through the compliance process established by the District Web Publisher (Web Master).
3. The District Web site and individual employee Web pages/blogs will not:
  - a. Contain public message boards or chat-room areas. However, employees may allow two-way communication on blogs or private message boards as a part of the classroom curriculum as long as the employee previews (moderates) and approves all blog comments before they are posted on the Internet.
  - b. Allow the display of unsolicited comments from the general public. Any solicited public feedback should be reviewed by the employee before posting. Any questionable or inappropriate content will immediately be removed by the employee, the Academy Web Publisher or by the District Web Publisher (Web Master) with no notification.

## G. DEFINITIONS:

As used in District Administrative Rule Acceptable Use Policy (Use of Technology Resources in Instruction), the following definitions apply:

“Blogs” (short for Web Logs) means dynamic web sites consisting of regularly updated entries displayed in reverse chronological order. They read like a diary or journal, but with the most recent entry at the top. Blogs can allow for open comments meaning other individuals can respond to a posted entry. Open comments is an optional feature for most blog Web sites.

“Chat Rooms” means a Web site, part of a Web site, or part of an online service, that provides a venue for communities of users with a common interest to communicate in real time.

"Cookies" means messages that may include personally identifiable information, which are stored in a text file and used to identify visitors and possibly prepare customized Web pages for them.

"DoS attack" means a denial-of-service attack designed to overload an electronic network with useless traffic and messages.

"Educational purposes" means it relates to curriculum and instruction, research, career or professional development, or administrative purposes.

"E-mail" means an electronic message generated using the District's e-mail and/or Web based e-mail. It is also used generically to mean either the District's e-mail system or a Web-based e-mail system.

"External site" means Web sites and materials not hosted on the District's Web server.

"Hacking" means the illegal activity of breaking into a computer system or electronic network, regardless of intent to cause harm.

"Inappropriate material" means material that does not serve an instructional or educational purpose and that includes, but is not limited, to material that:

- (i) is profane, vulgar, lewd, obscene, offensive, indecent, sexually explicit, or threatening;
- (ii) advocates illegal or dangerous acts;
- (iii) causes disruption to Cobb County School District, its employees or students;
- (iv) advocates violence; or
- (v) contains knowingly false, recklessly false, or defamatory information.

"Instructional activity" means a classroom activity that focuses on appropriate and specific learning goals and objectives.

"Message board" means a virtual bulletin board, where people post and view messages.

"Mirroring" means the creation of other Web sites that replicate or duplicate an existing Web site in order to reduce network traffic or improve performance and availability of the original Web site.

"Teacher directed" means that the teacher gives to the students' specific instructions for activities and assignments.

"Teacher supervised" means that a staff member will oversee the activities of the students.

"Technology" means but is not limited to electronic media systems such as computers, computing devices, peripheral devices, telecommunication equipment, electronic networks, messaging, and Web site publishing, and the associated hardware and software programs used for purposes such as, but not limited to, developing, retrieving, storing, disseminating, and accessing instructional, educational, and administrative information.



"Trojan Horse" means a destructive computer program that enters onto a computer by pretending to be a simple and safe computer application.

"Users" means Academy students, certain employees, including school and Central Office staff, and other authorized persons who use the District's technology.

"Virus" means a replicating computer program or piece of code that is loaded onto a computer without the user's knowledge and may attach itself to other computer programs and spread to other computers.

"Web Bug" means an invisible image placed on a Web page that is embedded in JavaScript code that collects information about a user's Internet behavior.

"Web Page" means a single document or file on the Web, identified by a unique URL.

"Web Site" means a collection of "pages" or files on the Web that are linked together and maintained by a company, organization, or individual.

"Worms" means a type of virus that can replicate itself and use a computer's memory but can or cannot attach to other computer programs.

## **Disaster Recovery**

The initial goal here was to create a comprehensive disaster recovery plan to ensure that the district's administrative and instructional computer systems are backed up.

The creation of this plan was recommended by the Academy Board of Advisors.

This plan takes into account many other areas that will need to be addressed in case of a disaster.

### **THE ACADEMY'S COMPREHENSIVE DISASTER RECOVERY PLAN**

#### **A. General**

##### 1. Definition

The purpose of this disaster recovery plan is to provide the necessary policies and procedures that would be followed in the event of a disaster which would provide a path to recovery.

2. Goal: to resume normal business operations in 48 hours.

#### **B. Advance Preparation and Emergency Response Phase**

1. Leadership: define a Disaster Recovery (DR) Team.

a. Membership.

- i. Superintendent of Schools
- ii. Assistant Superintendent of Curriculum & Instruction of Curriculum & Instruction
- iii. Director of Plant Services & Facility Planning
- iv. Chief Financial Officer
- v. Director of Human Resources
- vi. Director of Information Systems
- vii. Campus Principals
- viii. Network Administrator
- ix. Energy Management
- x. PEIMS Coordinator
- xi. Health Services Supervisor

### c. Duties

- i. Superintendent of Schools directs the Team; official spokesperson; “point person” to whom all information is reported; makes major operational decisions; consults with all members; assigns persons to the DR Team; delegates these tasks as appropriate.
- ii. Assistant Superintendent of Curriculum & Instruction: liaison with Superintendent of Schools. Performs Superintendents duties if not present, and/or delegates duties to DR Team. Fields all inquiries from media, members and the public; prepares official statements, talking points, and communication strategies and advises the CR Team on implementation. Disseminates information to the media and the membership. Refers interview and information requests to the designated official spokesperson.
- iii. Director of Plant Services & Facility Planning: activates the DR Team and facilitates meetings. Performs Superintendents duties as delegated if Superintendent and Assistant Superintendent of Curriculum & Instruction are unavailable. Confers with local fire and rescue teams, utility companies, etc. as appropriate to gather information; in charge of recovery of premises and physical property. Communicates with staff.
- iv. Director of Information Systems: insures that all network infrastructure and telecommunications are operational, provides information to the community via the website, and insures that all data is restored.
- v. Chief Financial Officer: ensures security of non-physical assets, availability of cash for emergency purposes; continuity of payroll and vendor payments. Provides liaison with insurers.
- vi. Director of Human Resources: maintains a current list of employees and ensures they receive appropriate information and duties.
- vii. Campus Principals: responsible for assessing situations at their assigned campus and reporting this information to designated members.
- viii. Network Administrator: ensures that all necessary servers are operational and verifies what data needs to be restored if any.
- ix. Energy Management: verifies that all areas of energy management are operational.

x. PEIMS Coordinator: verifies that all student data is correct and notifies network administrator of any data loss so that a restore from backup can occur.

xi. Health Services Supervisor: ensures that adequate first aid materials are on hand at necessary locations.

2. Emergency equipment

- a. First aid kit(s)
- b. Flashlights, batteries, rescue and escape equipment (as appropriate)
- c. Backup communications, cell phones, radios, etc.

3. Where to meet

In preferred Order:

- a. Central Administration
- b. Rockport Elementary/Community Center
- c. Auditorium
- d. Middle School Library

4. Communications: inbound and outbound

- a. Initial (inbound) alert: Superintendent will identify a person, with a phone/e-mail/desk location where news of a crisis and subsequent developments should be reported.
- b. Outbound: Superintendent will identify the person responsible for calling fire, police, rescue, and related services; list the numbers to call.
- c. Web posting.
- d. E-mail
- e. Broadcast media

5. Communications: notification chain

- a. Employees

1. All Department Heads should be notified immediately by the campus principal or other designated person

2. Department Heads are responsible for notifying their peers in a phone chain.
3. The phone numbers and e-mail addresses of every employee, as well as an emergency contact person, with phone and e-mail, for each employee can be obtained from the Director of Human Resources.

b. Officers and Board

1. Any officer who is on the DR Team must be notified at once.
2. The School Board should be notified as promptly as possible, so that they are informed and ready to convene and make decisions if necessary. In particular when the scope of the emergency and recovery schedule are known. If the DR Team have the proper authority in advance, immediate action by the Board should not be needed.

- c. Meeting registrants and other members currently engaged in association activities Meetings or other activities underway or scheduled in the near future, will need to be addressed and a designated person should communicate information about continuation, postponement, or cancellation as soon as the decision is made.

d. Media

A proactive approach to the media, rather than waiting for calls to come in

6. Escalation of alerts in the event of potential terrorist action

Green (low risk): routine maintenance of Plan

Blue (guarded risk): routine maintenance of Plan

Yellow (elevated risk): review Plan; ensure all data is current and emergency equipment is functional.

Orange (high risk): review as above; also check staff schedules and availability of DR Team and backups

Red (severe risk): Convene and brief DR Team

7. Rest and Recovery

The DR Team must pay attention to the physical and emotional needs of those who are engaged in the emergency and recovery. People perform less efficiently after only a few hours without food and beverages, and after 8-10 hours of continuous stressful activity without a break and rest. Availability of refreshments, food, washrooms, and places to rest is very important and should be on the agenda at each meeting of the Team during crisis recovery. A Team member should be assigned to locate these kinds of facilities early in the recovery process.

## 8. Districts Role in Community Recovery

Superintendent may designate employees of our district that have necessary skills, to assist with the community's recovery.

### **C. Business Recovery Phase**

DR team will work together to roll out a plan for school to start back up.

#### 1. Computing facilities and data

Hardware: The Director of Information Systems will secure computer equipment for necessary operations and identify staff laptops and home computer equipment which can be brought on-line immediately, and secure staff consent to do so; if necessary, identify vendor(s) who are willing to provide temporary computers, servers, and networks.

Software: extra copies will be stored offsite along with a list of all software licenses and vendor contacts.

Data: Backup's are done on a daily basis by the technology department. Backups are kept for three weeks before cycling of the tapes takes place. The Network Administrator is the primary contact for backup inquiries.

#### 2. Office space

A temporary headquarters will be designated by the Superintendent of Schools

#### 3. Office equipment: copiers, fax service, furniture, desk supplies. These items should be acquired and placed as needed.

#### 4. Telephone service

This is vital to communications; temporary lines may need to be established at the designated headquarters. These numbers should be publicized as needed. This responsibility lies with the Director of Information Systems.

#### 5. Mail and Package Delivery

US Postal Service, FedEx, UPS, and other delivery services should be notified about how to make deliveries during the emergency and recovery, which will require review in an actual emergency before issuance.

#### 6. Bank Authorizations

Chief Financial Officer will handle the transfer and withdraw of funds, and the written authorizations.

#### 7. Payroll Service

Employees should be notified how they will receive payroll ASAP to prevent panic.

#### 8. Insurance Vendors

A designated official will maintain a copy of up to date policy numbers and contacts for the association's property and casualty, life, and health insurance policies

## **D. Implementation**

### 1. Pre-Issuance Reviews and Updates

- a. Policies and Procedures are current and appropriate.
- b. Emergency funding can be secured.
- c. Emergency equipment is in place and functional.
- d. Backups for equipment, software, data, and office facilities have been arranged.  
Keys and combinations are secure, but available off-site, and locations are known to key persons.

### 2. Plan Distribution

Superintendent, along with the entire DR team, will decide who will receive what parts of the plan to implement if it is not specifically noted in the plan.

### 3. Briefing and Training

Superintendent or designated official will ensure that every staff member and key officer knows his/her part in the Plan. Discussion in a one-on-one or small group format will help ensure that all staff are informed and prepared, and will also reveal areas in which the Plan can be improved; specific training needs, such as where fire exits are, availability of staff with CPR and first aid qualifications, etc.

### 4. Practice Drill/Walk-through

A practice drill should be carried out at least once a year to insure plan is complete and to make additions or modifications as needed.

### 5. Reviewing, Evaluating, and Updating

A meeting of the DR team should occur once a year to review, evaluate and update the plan

## **E. Appendix**

### 1. Disaster Recovery Team Roster

Superintendent of Schools –  
Assistant Superintendent of Curr & Instruction–  
Director of Plant Services & Facility Planning –  
Chief Financial Officer –  
Director of Human Resources –  
Director of Information Systems --  
Campus Principals –  
Network Administrator –  
Energy Management -  
PEIMS Coordinator –

Health Services Supervisor –

2. Employee Roster

Provided and maintained by Director of Human Resources

3. School Board

President

Vice-President

Secretary

Member

Member

Member

Member

4. Phone Chain

5. Suppliers for Building Maintenance and Repair.

Vendor list maintained by the Director of Operations

6. Suppliers for all Office Furniture, Equipment, Computing Systems, Software, Accounting and Payroll Services, Office Supplies, etc. List is maintained by the Chief Financial Officer

7. Dealing with Emergencies at Events.

Staff designated by the Superintendent



## **Disposal and Repurposing Policy**

The Academy has a responsibility to uphold the public trust. Protection of District assets per Board Policies purchased with public funds is one way the District seeks to uphold this trust. The Academy fulfills the requirement in Georgia law which requires its approval for district property to be designated as surplus under O.C.G.A § 20-2-520.

### **RULE:**

#### **A. SURPLUS PROPERTY:**

##### **1. Classification:**

An item is classified as surplus after it has been submitted to the Board for disposition and the Board approves the classification;

##### **2. Sale:**

When the Board classifies property as surplus:

- a. The Director of Procurement Services shall have the authority to proceed with offering the surplus items for sale to the public;
- b. Surplus items may be sold by sealed bid, public auction, private sale, on-line auction, or negotiated contract, whichever is in the best interest of the District;

##### **c. Employee Exclusion:**

District employees empowered with the responsibility of identifying potential surplus items will be excluded from:

- (1) Bidding on the items they identify; or
- (2) Otherwise benefiting from the disposal of any surplus property.

##### **3. Unsold Items:**

Surplus items that do not sell and have an estimated value of less than \$5,000 shall be disposed of in a manner most beneficial to the District by the Director of Procurement Services.

##### **4. Exception for Unsafe Items:**

The Director of Procurement Services shall:

- a. Determine the most efficient manner to dispose of surplus items that pose an immediate health or safety risk to the District; and
- b. Report the disposal of property under this exception to the Board at its next scheduled meeting for their approval

##### **5. Proceeds:**

Funds received through the disposal of surplus items will be reported to the Board.

#### **B. CONFISCATED/LOST PROPERTY:**

##### **1. Department of Public Safety:**

Confiscated items received by the Department of Public Safety should be processed utilizing the guidelines contained in:

- a. The Department of Public Safety Department Manual; and
- b. Administrative Rules, unless a longer period of time is necessary due to administrative hearings;

##### **2. Unclaimed Items:**

Confiscated items held by the Department of Public Safety and confiscated/lost items

held by schools that remain unclaimed may be declared surplus property and may be sold or disposed of in the best interest of the school or District.

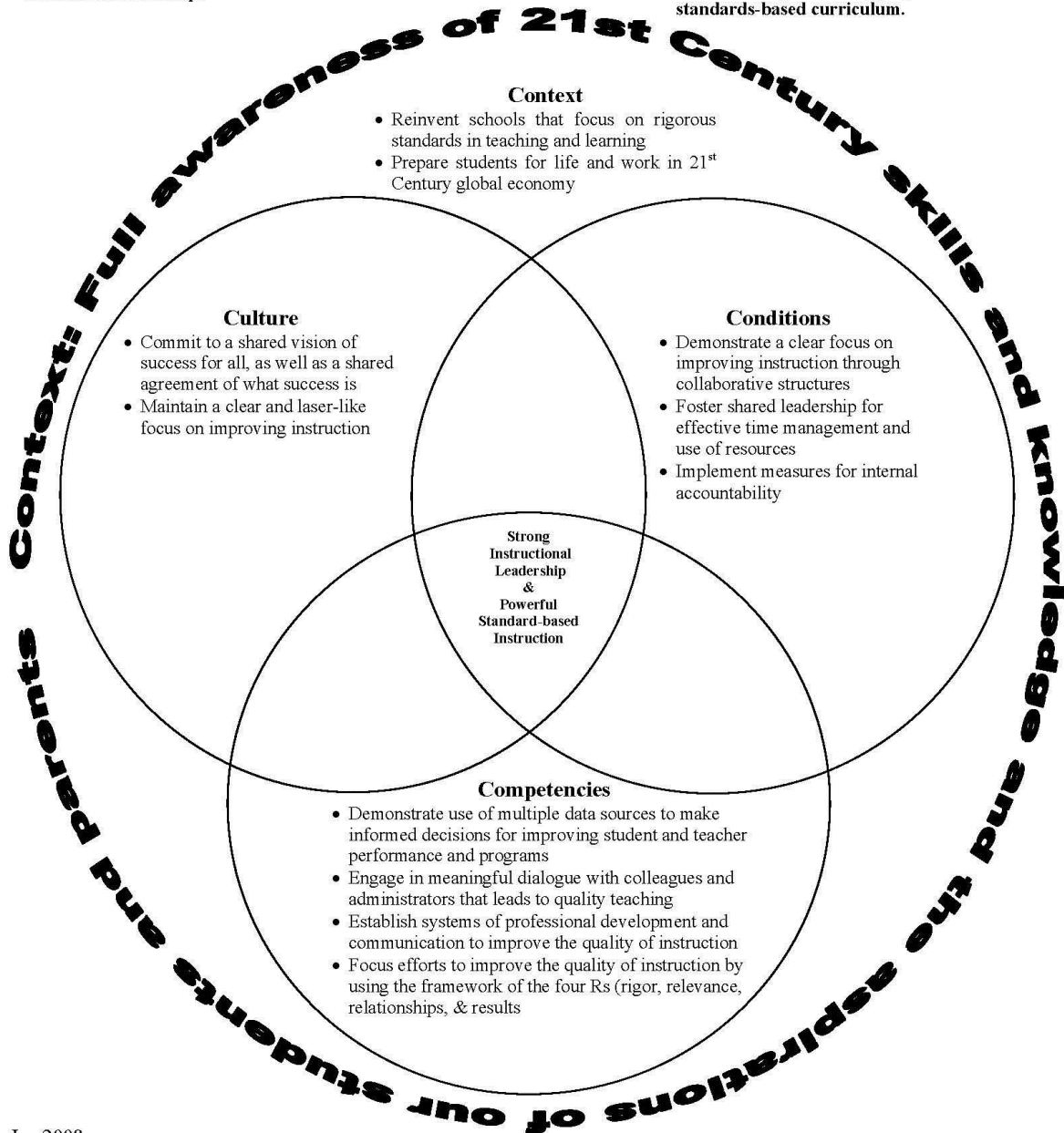
In addition to the above listed policy, technology deemed still operable by the Chief Technology Officer may be repurposed for use in other areas or schools. This is especially important with respect to computers and laptops. While they may no longer be under warranty, we will support them on the network as long as feasible. Equipment over 7 years old will be disposed of in accordance with the above procedures.

## Professional Development Plan for Teachers and Administrators

Administrators will lead schools in developing capacity for creating and sustaining continuous learning communities and a culture of collaboration through distributed leadership.



Administrators and teachers will participate as collaborative and continuous learners in their school settings to extend their knowledge base and expand generic and content specific instructional practices appropriate for standards-based curriculum.



Jan 2008

Framework from Change Leadership: A Practical Guide to Transforming our Schools by Tony Wagner and Robert Kegan

All training and professional development will take place within the context of the model outlined above. Teachers will endeavor to engage in ongoing professional development and education that provides them with content rich activities which translate well into the classroom. The demonstration by our educators of a lifelong love of learning will help inspire our students to learn as well. With this in mind the following guidelines will apply:

1. Teachers will engage in a minimum of 10 hours of technology training per year, 5 of these will be mandated by the Academy, while 5 others will be selected by the teacher.
2. All hours offered will be during professional development time provided for in the school schedule and during teacher workdays. The district will offer adequate classes to allow for choice.
3. To ensure that technology is being utilized adequately, evaluators will be looking at its use in lesson plans and during classroom observations as part of the teacher's annual evaluation.
4. The district will provide instructors for courses from within the district, from professional outside resources, and utilizing volunteers from local universities and colleges.
5. Teachers will be encouraged to attend workshops and trainings outside of the district offered courses, and for those where a stipend is not offered, basic costs will be covered as long a budget allows.
6. You are all encouraged to volunteer at local teacher training events and workshops.
7. Teachers who pursue post graduate educational opportunities outside of the professional development offered will be assigned a pay increase based on level of education and within budgetary parameters.