

Effective Date: _____

Approved by: IT Management

Revision Date: _____

Title: IT.ITMGT.007.S01 Technology Guidelines and Procedures

Purpose: To provide access to customers for requested technical support from IT.

Scope: This applies to the Department of Instructional & Information Technology guidelines & services offered

Guideline: Customer may find technical support and technology guidelines as it relates to district approved technology

Memphis City Schools



Technology Guidelines and Procedures

Department of Information Technology
and
Department of Curriculum & Professional Development

July 2008

Table of Contents

Introduction.....	3
Help.....	3
Copyright Guidelines	4
Purchases	4
Grant Applications	5
Donations	6
Security	6
Hardware Maintenance	8
Inventory	9
Training.....	11
E-Mail	12
General Network Cabling Requirements.....	13
Electrical Outlets.....	18
Wireless Technology	18
Video Conferencing.....	18
Video/Audio Streaming	19
Switch Equipment.....	19
Workstations	20
Network Connectivity – Hardware	20
Network Connectivity –Wireless.....	21
Point-Of-Service	21
SIS Hardware	21
Miscellaneous Hardware.....	21
Software	22
Appendix A.....	27
Appendix B	38
Appendix C	42
Appendix D.....	44
Appendix E	65
Appendix F.....	67

Memphis City Schools

Technology Guidelines and Procedures

Introduction

This document was created jointly by the Department of Information Technology and the Department of Curriculum and Professional Development. The purpose of this document is to provide district-wide guidelines and procedures for administrative and instructional technology.

This printed document is updated annually. As new guidelines or procedures are created, they will be posted on the web at <http://www.mcsk12.net/admin/it/itweb/pdf/techguidelines.pdf>.

Help

General Technical Help

The Memphis City Schools Support Center, 416-2700, is available for technical assistance for telephone, hardware, and software problems and is responsible for documentation and resolution of all calls received. Application support is also provided by Easy IP for Exceptional Children and Mental Health. Student Information provides support for Chancery SMS at 416-6649.

System Assistance/Request for Support

The following guidelines are for approved and funded projects only. All telephones, hardware, and software must be installed to meet MCS guidelines. For assistance with new or modified networked systems and major technology planning, a Request for Support, MCS 028, must be completed with the latest electronic form found in the Support Request Lotus Notes database. The completed requests may be prioritized by Executive Staff. A site visit from the staff of Information Technology and/or the staff from Network, Wiring, and Cabling may be made to assist with:

- Explanations of technical concepts, as needed
- Training needs
- Equipment and installation requests
- Security Authorization Requests
- Cost estimates

MAC is an acronym for the words Move, Add, Change. Customer requests that require:

- moving something that already exists,
- adding something new to a service that already exists, or
- changing an existing service.

All MAC's require the submission of a Request for Support, MCS 028, electronic form found in the Support Request Lotus Notes database. Requirements will be gathered and a price quotation provided for the principal's/director's review and funding approval.

Copyright Guidelines

All MCS personnel will:

- Be knowledgeable of the law which states it is illegal:
 - * To use MCS equipment to make illegal copies
 - * To use illegally copied software
 - * To use multiple load software without written permission
 - * To use software on a networked system without written permission
 - * To use software obtained from the MCS district site licensing outside of the system
- Set an example of compliance
- Insist others comply with the law
- Purchase materials in sufficient quantities to preclude the need for illegal software copies
- Observe software licensing agreements of copyright holders

It is required that the following information be posted in prominent locations throughout the site.

MANY COMPUTER PROGRAMS ARE PROTECTED BY COPYRIGHT. 17
U.S.C.\S\101. UNAUTHORIZED COPYING IS PROHIBITED BY LAW AND
PUNISHABLE BY FINE, IMPRISONMENT, OR BOTH. (See Appendix E)

There are numerous websites and books available which provide detailed copyright information.

Simpson, Carol Mann. *Copyright for Schools: A Practical Guide, 3rd. Ed.* Ohio: Linworth Publishing, Inc., 2001.

Bruwelheide, Janis H. *The Copyright Primer for Librarians and Educators.*
Chicago and London: American Library Association and Washington, D.C.: National Education Association, 1995.

United States Copyright Office, <http://www.copyright.gov>

Lesley Ellen Harris website, <http://copyrightlaws.com>

Library of Congress, "Copyright Basics," United States Copyright Office, July 2006,
<http://www.copyright.gov/circs/circ01.pdf>

O'Mahoney, Benedict. *The Copyright Website*, <http://www.benedict.com>.

Purchases

Requisitions

The MCS website, http://www.mcsk12.net/aboutmcs_procurement_services_computers.asp, should be referenced for "Desktop PC and Notebook" purchasing information and "Information for completing Apple Requisitions." This resource provides information on currently supported hardware (desktops, laptops, and servers) and software. Configurations are maintained for both instructional and administrative systems in the PC and Apple product families. Installation is included in prices and is the responsibility of the installing vendor. The Master PC agreement is

posted annually for bids. The bid is awarded to vendors in three categories: Desktop, Laptop, and Tablet. For server purchases, contact the Information Technology Department for assistance.

The principal or division director must ensure that sufficient network connections are available for any new equipment purchased. If additional connections will be needed, a Request for Support, MCS 0028 form, must be completed with the latest electronic form found in the Support Request Lotus Notes database. The Request for Support form should be submitted with appropriate budgetary coding and the principal's/director's approval. **Computers should not be ordered assuming that wireless or hubs/switches will be used for connectivity.** See sections on Wireless Technology and Switch Equipment later in this document for information on restricted use of this technology.

When schools make instructional technology purchases, they are to submit a School-Level Technology Project Worksheet (Appendix A, MCS-0055) to the Department of Information Technology, Room 250, along with the Purchase Requisition for approval. This form is located at <http://www.mcsk12.net/admin/it/itweb/pdf/MCS0055.pdf>.

Nonstandard Products

If a product is not a District standard, the requisition must be submitted with a Nonstandard Purchase Form (Appendix A, MCS-0047). **Nonstandard equipment will not be allowed on the MCS network without specific written approval of the Chief Technology Officer.**

Large Purchases

Individual items that are \$25,000 or more must be approved by the Board of Commissioners prior to purchase. Contracts, leases, professional services contracts, and lease/purchase contracts totaling \$50,000 or more must be Board approved. Purchases whose line item total equals \$50,000 or more must have Board approval prior to purchase. These line items must have a "Service/Materials Justification Form." This form may be obtained from the Procurement Services or duplicated from the sample in Appendix A. As detailed in the "Requisitions section", instructional purchases must also have a School-Level Technology Project Worksheet (Appendix A, MCS-0055).

Grant Applications

Technology hardware, including servers, and software included in grant applications must include any necessary computer drops, electrical outlets, and wiring closet electronics, unless precluded by funding source, and must be explained in the grant proposal brief submitted to the Grants Office. A review of the proposed technology by Information Technology is highly recommended to ensure that all requirements needed to implement the proposed technology are accurately identified and priced. Include the deadline date for encumbering grant money when submitting the Request for Support, MCS 028, electronic form found in the Support Request Lotus Notes database. The request should be completed to allow as much lead time as possible. [For servers, this means a minimum of three (3) months.]

Donations

Guidelines for Acceptance

Often businesses contact schools offering to donate old computer equipment that may or may not be usable in a school environment. For advice on acceptable donated equipment, contact the MCS Support Center, 416-2700. Certain **minimum** specifications are necessary because of current software requirements, connectivity and performance issues, and vendor support availability. Below are guidelines for accepting donations. These guidelines ensure that the equipment can be used on MCS networks. MCS is unable to maintain the staff and expertise necessary to provide service for equipment that does not meet these guidelines. The site is responsible for submitting a MCS Equipment Transfer Form No. 14671 to Inventory Control to have all donated equipment tagged.

If the computer is to be included on the MCS instructional network, a Wake-on-LAN capable PC and Ethernet network adapter is required. For APPLE computers, an APPLE compatible 10/100 Base-T Ethernet adapter must be included.

NOTE: MCS does NOT provide hardware for donated equipment. Support of District standard software is available. (Note: You must purchase a product license before installation of Microsoft Office Suite.) See Software section (page 21) of this document.

For Instructional purposes:

Minimum requirements include: PC Platform (IBM, Dell, Gateway, HP-Compaq) – P4 and above with 800MHz processor, 128MB RAM, 20 GB hard drive, Windows 2000 or Windows XP Professional OS with License. (Windows XP Home Edition does NOT meet minimum requirements.)

APPLE – G4 class processor (or higher) with 128MB RAM and 20 GB hard drive running OSX (10.2) as well as Classic (Mac OS 9.2.2)

For Administrative purposes:

Due to centralized monitoring and control of administrative software and hardware, donated equipment will not be allowed on administrative networks without the prior approval of the Chief Technology Officer.

Security

Hardware Security

New Equipment

Single-unit locking devices are included in configuration pricing on the MCS website. Additional security for all new equipment is the responsibility of the Principal or division head.

File Servers

File servers will be located in a secure non-public place with no outside windows when possible.

- Single-unit locking devices are required for all servers.
- Access to the file server will be limited to approved personnel ONLY.

Workstations

Workstations and printers used to display sensitive information should not face a counter or public area. Workstations and printers must be secured with approved security cables. Single-unit locking devices are required. Information Technology may install software or change configuration settings on all machines attached to the network in order to keep them up to date with security and system patches.

Software Security

Alteration of Software

- MCS-developed software will be altered ONLY by authorized Information Technology personnel.
- Packaged software (purchased software, not written or maintained by Information Technology personnel) will not be altered.

Storage of Software

- Original media (diskettes, CD's, Zip Disks, USB drives, etc.), and backup copies of packaged software must be stored in a secure place at the local site away from dust, temperature extremes, and magnetic fields, e.g., telephone, and will be accessible to key authorized personnel ONLY.
- A library of backup copies of all versions of MCS-developed administrative software currently in use will be maintained in the Department of Information Technology.

Data Security

Sensitive Data

- Highly sensitive printouts and/or other media must be disposed of in a secure fashion, e.g., shredding, shred bins, or other means of physical destruction.
- Sensitive data that needs to be transmitted outside of the District's network should be done in a secure manner. Sensitive information, including student and personnel records, should not be transmitted outside of the District via e-mail under any circumstances. Please contact the Department of Information Technology for assistance.

Administrative Systems

- Principals must submit Security Access form (Appendix A, MCS-0034) to the Office of Student Information requesting access to the Student Information System.
- MCS-0035 (Appendix A, MCS-0035) must be used to request User ID's.
- Passwords will be activated on all local area networks.
- Information Technology will enforce password security and will immediately revoke the password of a terminated employee upon notification by the principal/division head.

- Within the area of microcomputer software resources, data access, e.g., directories, files, records, fields, will be restricted to ONLY the necessary data required for a particular job.
- Students/non-MCS employees should not be allowed access to administrative computers.

Network Security

- Network security includes servers, PDA's, laptops, workstations, servers, and any devices attached to the MCS network.
- Non-MCS Internet access, such as cable modems, dial-up, DSL, etc., is not allowed at MCS sites.
- Users must log off the network before leaving a workstation unattended. Failure to do so may result in loss or corruption of data or software. Information Technology will not be responsible for recovery.
- Wiring closets contain the switches and other equipment that keeps the network running, and it is critical that they be kept clean and safe. Access must be limited to only authorized Information Technology support personnel and the building engineer. Connections to equipment in the wiring closet are to be made only by Information Technology support staff. Wiring closets should not be used for other types of storage.
- Connections needed for energy management, wireless access, emergency equipment, etc., must be reviewed and approved by Information Technology.
- Wiring closets must not be used for storage of cleaning equipment or anything else. Likewise, they must not be used for housing workstations, servers, or other equipment.

VPN Access

For users requiring external access to internal resources, VPN (Virtual Private Network) solutions are available. Users who need VPN access should fill out the VPN access form (Appendix A, MCS-0054), and submit it to Information Technology for approval.

- Multiple users requiring access to a single application will be given access via SSLVPN.
- Individual users requiring access to multiple resources will be given access via client-based VPN.
- Accounts that expire after 60 days of inactivity will be deleted and must be reapplied for.

Hardware Maintenance

Hardware Alteration

Computer hardware (including hardware configuration) will ONLY be altered by:

- Authorized Information Technology personnel
- A vendor with approval from Information Technology management

Repairs

Users are responsible for the repair of all non-warranty equipment. Users may contact the MCS Support Center, 416-2700, for assistance in confirming warranty status and/or locating a repair center for the non-warranty equipment. (See Appendix C for procedures.)

Warranty

Warranty is the responsibility of the user and should be purchased for all equipment. A three-year warranty is automatically added to computer purchases by the Procurement Services Division. This is included in the purchase price. The user will be responsible for budgeting the necessary funds to cover extended warranties. It is the user's responsibility to purchase services and parts to repair non-warranty equipment. Warranty repair service is the responsibility of the vendor for the first three (3) days from the date delivered. After the third day, call MCS Support Services at 416-2700 for repairs.

Obsolete Equipment

Computers and related equipment seven (7) years of age will be considered obsolete. Schools should seek to obtain replacement for and retirement for the equipment as soon as possible.

Supported Apple Equipment

All Apple equipment, not still under manufacturer warranty, will only receive software support through Information Technology. For support, contact the MCS Support Center at 416-2700.

Supported PC Equipment

Approved PC vendors are Dell, Gateway, HP/Compaq, and IBM. The minimum systems specifications are the *same* as donated equipment.

Information Technology no longer provides support for Novell NetWare.

Laptop Computers

The user must transport the laptop computer to the vendor for repair. Contact the MCS Support Center, 416-2700, if assistance is needed in finding a repair facility. Any repairs made to laptops no longer under warranty are at school or administrative office expense. The user makes payment arrangements to the vendor at time of service.

Moving Equipment

For information, contact MCS Support Center at 416-2700 BEFORE moving local area networks and/or computers with hard drives to another MCS site. This equipment must be properly disconnected. The physical move of equipment is the responsibility of the school/site.

Inventory

Hardware

- All equipment is received, inventoried, transferred, repaired, and disposed according to MCS Procedures (Appendices B and C).
- An official copy of hardware inventory is maintained at the site and at Division of Inventory Control and Warehousing.

Installation and set-up services for Servers and Standard CPU's

Vendors are responsible for:

- Preparing Computer Equipment Delivery Receipt
- Unpacking from shipping containers at the setup location
- Setting up the CPU and attaching the display, keyboard, mouse, and power cords
- Installing any add-ins, such as memory, or network interface cards
- Installing any system software, MCS image, and testing functionality
- Setting up standard MCS user accounts
- Setting up, connecting, and testing peripherals (printers, scanners, etc.), and accessories to the computer
- Connecting and testing the CPU and/or peripherals to a Local Area Network (LAN) or Ethernet outlet at the desktop
- Verifying that the CPU and peripherals are operational on MCS LAN and WAN
- Notifying the customer that the system is ready to use (signed release from site)
- Moving packing material and product boxes for disposal to an MCS designated on-site location
- Ensuring that equipment is tagged and the Equipment Transfer forms are sent to the Division of Inventory Control and Warehousing

Installations do not include:

- Staff development necessary for maintaining instructional network file servers
- Setting up, installing, or maintaining third party hardware or application software not included in the contract
- Loading and converting customer data or electronic files unless contracted
- Troubleshooting or repairing network issues
- Network administration, such as setting up files sharing or passwords on file servers. Contact the MCS Support Center, 416-2700, to request this service.

Software Maintenance

System Backups

Administrative and Instructional system backups will include:

- Daily data backups **by user** with a minimum of two (2) weeks of backup to be used alternately (e.g., Plato Labs, any other school-based networked application).
- User is responsible for ensuring complete system backups at time of initial installation and at each software upgrade revision.
- Student Information System and Atrium backups will be maintained centrally by Information Technology.

Hard Drive Management

Users are responsible for maintaining their individual workstation data and performing data backups to a storage media. Users may contact the MCS Support Center at 416-2700 if assistance in data backup procedures is required.

Virus Protection

- All new computer purchases include virus detection software. The virus protection software is bundled with the purchase price of every new computer.
- Virus detection software is **REQUIRED on ALL** machines and can be purchased separately for existing computers. Please refer to Procurement Services Division website: http://www.mcsk12.net/aboutmcs_procurements.asp.
- **Detected viruses must be reported to the MCS Support Center, 416-2700, immediately.**
- **Infected computers and/or entire sites may be disconnected from the MCS network during virus outbreaks.**

System Changes

- System software will only be altered by authorized personnel from the Department of Information Technology.

Instructional Applications

- Installation of any instructional application and related plug-ins (stand alone or network) should be contracted with the vendor at the time of purchase. Otherwise, the school is responsible for resources and installation of the application.
- Schools are responsible for staff development necessary to maintain network software applications (Plato, Renaissance Learning Products, Riverdeep, etc.).
- Maintenance and support contracts must be purchased from the vendor for all instructional network applications (Plato, Renaissance Learning Products, Riverdeep, Read 180, etc.).

Utilities

Utility software (e.g., FoolProof, Deep Freeze, and Norton Disk Doctor) will not be used on any computers without prior approval from Information Technology Customer Support management. A Request for Support, MCS 028, must be completed with the latest electronic form found in the Support Request Lotus Notes database, to request installation of any non-standard utility software.

Training

Since the District's strategic goal embraces a system of accountability for high-quality and professional learning, this component must be passed along to employees also. It is identified as professional development and is offered at two basic levels: instructional and administrative.

Instructional

All professional development for teachers to integrate technology in the classroom is offered at the Teaching & Learning Academy located at 2485 Union Avenue. These sessions are listed online in the PDMS Class catalog and updated on a regular basis. Special training schedules are posted on the TLA web pages as they become available.

Registration is also handled through the MCS Professional Development Management System (PDMS). The PDMS maintains easy access to training records for electronic reporting purposes and concerns.

Administrative

As the need for professional development for administrative staff continues to expand, the school district provides opportunities for continuous improvement and more job-embedded training. The Department of Human Resources publishes a catalog of multiple training opportunities for all classified personnel. The sessions may be housed at various locations including the Messick Training Center (703 South Greer) and the Technology Training Center.

The Technology Training Center (TTC) offers administrative computer training, on a regular and special-request basis, at 3772 Jackson Avenue. Administrative application training includes: SMS/Chancery, Parent Link, Intro to Personal Computer, Windows XP, Lotus Notes, Lotus Domino Web Access E-mail, Microsoft 2007 Professional Office Suite (Access, Excel, Word, PowerPoint, and Publisher), and many others. A complete listing of classes can be viewed on-line from the MCS website's home page via the TTC Classes Catalog using the following link: <http://www.mcsk12.net/admin/it/ttc/pdccatalog.html>. Additionally, open labs are available to provide a quiet, comfortable place to work, and immediate assistance is offered, if requested. The TTC facility is available to all MCS departments to assist with specific computer training needs.

Registration is handled online using the TTC Classes Catalog. Contact the Technology Training Center at 416-4207, for additional information. The facility's office hours are Monday-Friday, 7:30 a.m. - 4:45 p.m.

E-Mail

E-mail will be provided to administrative and instructional staff via Lotus Notes. Every effort is made to filter spam; however, in order to ensure that legitimate e-mail is not filtered, spam may be delivered to a user's account. E-mail accounts other than Lotus Notes are not authorized for use on the MCS network.

For Internet and e-mail access, an Acceptable Use Agreement must be signed by the user and kept on file at his/her site. Access will be terminated promptly when an employee leaves the MCS system or violates the Agreement.

All files, Internet use, and e-mails are subject to review at any time by MCS.

Instructional

Domino Web access e-mail is available to all teachers. Optional training is available at the Technology Training Center, 416-4203. On-line registration is available at <http://www.mcsk12.net/admin/it/itweb/pdf/MCS0053.pdf>.

Any access to the MCS network must be approved by the principal based on MCS instructional and/or administrative policies, regulations, and guidelines.

Administrative

The Department of Information Technology manages the Memphis City Schools mail servers. Accounts are assigned by this Department and may be obtained upon completion of Lotus Notes training at the Technology Training Center. Lotus Notes client e-mail accounts are available to administrative personnel at the Avery location and sites connected to the Avery location.

General Network Cabling Requirements

All cabling requests require a Request for Support, MCS 028, the electronic form found in the Support Request Lotus Notes database. This form should be submitted with the appropriate budgetary coding and principal/division director approval. Installations will use Category 6 products that conform to TIA/EIA guidelines. To assure compatibility with equipment, the following materials, or their equivalent shall be used.

System Assistance/Request for Support

The following guidelines are for approved and funded projects only. All telephones, hardware, and software must be installed to meet MCS guidelines. For assistance with new or modified networked systems and major technology planning, a Request for Support, MCS 028, must be completed with the latest electronic form found in the Support Request Lotus Notes database.

The completed requests may be prioritized by Executive Staff. A site visit from the staff of Information Technology and/or Network, Wiring, and Cabling Division may be made to assist with:

- Explanations of technical concepts, as needed
- Training needs
- Equipment and installation requests
- Security Authorization Requests
- Cost estimates

MAC is an acronym for the words Move, Add, Change. Customer requests that require:

- moving something that already exists,
- adding something new to a service that already exists, or
- changing an existing service.

All MAC's require the submission of a Request for Support, MCS 028, electronic form found in the Support Request Lotus Notes database. Requirements will be gathered and a price quotation provided for the principal's/director's review and funding approval.

NETWORKING CABLING MATERIAL

Item	Description	Spec #
A.	Systimax 6 Strand Indoor/Outdoor Fiber Cable	#5100-006A-XRBK
B.	Systimax 12 Strand Indoor/Outdoor Fiber Cable	#5100-012A-XRBK
C.	Systimax 24 Strand Indoor/Outdoor Fiber Cable	#5103-024A-XRBK
D.	Systimax 6-fiber fan-out kit for 6 & 12 LT cable	#F00-300-008
E.	Systimax 24 Strand Indoor/Plenum Fiber Cable	#5301-024A-XPAQ
F.	Systimax Plenum Cat.6 Giga speed cable (Orange)	#2071-004-AOR
G.	Systimax Plenum Cat.6 Giga speed cable (Blue)	#2071-004-ABL
H.	Systimax 25 pair Cat.3 Plenum Cable	#107765992
I.	Systimax 12/24 fiber mtg. shelf 600B2	#760028324
J.	Systimax 12 –fiber ST MM panel f/600B2	#760032151
K.	Systimax 24 –fiber ST MM panel f/600B2	#24ST1-EW
L.	Systimax fiber panel clear top cover	#184U1
M.	Systimax Quick Light MM ST connectors	#P2080A-Z-125
N.	Systimax 48 port Giga Speed Patch Panel	#760062380
O.	Systimax 24 port Giga Speed Patch Panel	#760062372
P.	Systimax 6 port Cat.6 module	#PM-GS3- Kit
Q.	Systimax 6 port MM ST fiber module	#DM2302ST/ST
R.	Systimax 110 Giga Speed Data Jack	#MGS400BH-246
S.	Systimax Faceplate 4 port	#M14L-246
T.	Systimax Blank Modules	#M81-246
U.	Systimax Dust Covers	#M21A-246
V.	Systimax Cat.6 Gray Patch Cables 8 ft.	#CPC3312-03F008
W.	Systimax Cat.6 Blue Patch Cables 8 ft.	#CPC3312-02008
X.	Data Box Plastic Deep	#Anixter 153940
Y.	Amp Cable Management Panel	#558331-1
Z.	19 in. EIA Rack Relay 84x 19 Hubble	#55053-703
AA.	19 in. EIA Rack Relay 96x 19 Hubble	#46353-515
BB.	Tele-communication Bus Bar CPI	#Anixter 123231
CC.	Cable Runway Ladder Rack (12 in. Wide Hubble	#10250-712
DD.	Cable Runway Support Kit (12 in. Wide Hubble	#HLX0612
EE.	Hubble Cable Management Panel	#HC219MS3N
FF.	Hubble Remote Equipment Cabinet	#RE2
GG.	“J” Hooks (16 cables Maximum)	#CAT-12
HH.	(50 cables Maximum)	# CAT-21
II.	(80 cables Maximum)	#CAT-32
JJ.	(Spes Seal fire stop putty or equal)	# N/A
KK.	Innerduct	#Anixter 127968
LL.	6 port Giga Speed module	#DM216065

- All data and voice jacks shall be RJ45 style (Systimax 110 Giga Speed data jack) using the four pair T658A wiring scheme.
- All data faceplate connections shall use the Systimax 110 style Giga Speed, eight-position data jacks.
- Dust covers will be furnished and installed in all data jacks in offices and classrooms.
- All penetrations of hallways and fire-rated walls shall be fireproofed with an UL-approved, fire-stop material.
- Cement or fireproofing that sets up hard shall be used around the outside of the conduit at all wall penetrations.
- Moldable fireproofing shall be used inside of conduit nipples.
- Arrange all computer cabling to interfere as little as possible with the school's normal operation. Existing computers will be moved by school personnel and shall not be moved by contractor.
- Identify all items of equipment installed on the project. Each faceplate cover, all cable ends, and patch panels shall be labeled with the cable type, room number, data/telephone cable number, and wire distribution rack, using a Kroy Dura Type 200 label marker or approved equal. Patch panels shall be marked to match the data/telephone cable number.
- Properly identify all wire distribution racks with black plastic plates with 1/4" white engraved lettering on the face of each, permanently attached with two tapped screws. Example: MDF.
- A label with the term Cat.6 shall be applied in the center of the Giga Speed patch panel. Each port in the six port modules shall be labeled to match the data/telephone cable numbers.
- Example of room labeling:
 - a. Room #301-#1-MDF
 - b. Room #301-#2-MDF
- Example of how to follow existing cable numbering sequences already established in rooms:
 - a. Room #301-#6-MDF (This is the last existing cable for room #301 in the patch P panel.)
 - b. Room #301-#7-MDF (This is the first new cable for room #301 added to the patch panel.)
- Example of how to label administration areas that are not assigned room numbers but use the abbreviation for "office":
 - a. Off.-#4-IDF#3
 - b. Off.-#5-IDF#3
- Example of how to follow existing cable numbering sequences already established in administration areas:
 - a. Off.-#6-IDF#3 (This is the last existing cable in office area in the patch panel.)
 - b. Off.-#7-IDF#3 (This is the first new cable added to office area in the patch panel.)
- Plenum grade cable shall be used in all indoor installations.
- All cable shall be concealed in the drop ceiling and walls when possible. Exposed cable that is not above drop ceiling shall be installed in EMT conduit raceway unless approved by the MCS Information Technology representative.
- Cable run above the drop ceiling shall be supported up and off the ceiling using "J" hooks alternated at three and four-foot spacing throughout "J" hook installation. Do not use equal spacing of "J" hooks or exceed four-foot spacing maximum on installation. All "J" hooks shall be supported from the building structure.
- Insulation Displacement Contact (IDC) shall be the method of termination the Cat.6 data jacks.
- All cable shall comply with the TIA specifications TSB40; cable bend radii shall not be less than eight times the cable diameter. This requirement translates to a minimum bend of two (2) inches.

- The contractor shall test all Cat.6 and Fiber optic cables and submit performance verification on disk (soft copy only). The contractor shall test all newly terminated cables using one of the following Fluke meters: model 4000, 4100, or 4300. All UTP cable shall meet the performance guidelines for Cat.6 cable and the MCS Information Technology standard of more than 3db headroom on cables.
- Cabling contractor shall submit to MCS proof that each cable installer and person testing cables has successfully completed a training class recognized by Building Industry Consulting Service International (BICSI) for installing and testing Unshielded Twisted Pair (UTP) Cat.6 cable.
- Fiber optic cable shall be installed in rigid conduit outside of building or messenger supported when aerial pathways are needed.
- Fiber cable run above the drop ceiling shall be supported up and off the ceiling in inner duct supported from the building structure and marked every 20 feet.
- Exposed fiber cable that is not above the drop ceiling shall be put in EMT raceway unless approved by MCS Information Technology representative.
- Fiber cable run between wire racks shall be FDDI certified 62.5/125 micron multimode cable.
- Fiber cable run to portable buildings shall be 6-strand indoor/outdoor fiber cable FDDI certified 62.5/125-micron multimode cable.
- Fiber cable run to portable buildings shall be run so that if a portable building is removed it will not affect other fiber runs.
- 24-strand fiber cable does not require inner duct. All other specifications apply.
- All fiber connectors shall be ST type.
- Contractor shall guarantee all strands of fiber not to be more than 3db loss.
- Rack mount fiber patch panels shall be used in wire closets.

SECURITY CABLING MATERIAL

Item	Description	Spec #
A.	Anixter/Belden CCTP Cable	CMP-422-7B-08-CCTP
B.	Anixter/Belden Jack	JCK 6-CCTP
C.	Anixter/Belden Patch Panel-16 port	16P6-CCTP
D.	Anixter/Belden Patch Panel-17 port	17P3-CCTP
E.	Anixter/Belden BNC Patch Panel	BNCP-160-CCTP
F.	Avaya 110 Block 50 pr.	245631
G.	Anixter/Belden BNC Patch Cable	BNCC-7-08-CCTP
H.	Anixter/Belden Patch Cable	SPC-5-08-CCTP
I.	Anixter/Belden CCTP 25 pr. Cable assembly	TR-25-3008-CCTP
J.	Anixter/Belden Jack Faceplate	01-FP-CCTP
K.	Anixter/ Belden #18 - 9/C Cable	B6307FE – 1000
L.	Avaya Plenum Cat.6 Giga Speed Cable (White)	# 2071-004-WH
M.	Avaya 25 pair Cat.3 Plenum Cable	# 107765992

- **CCTP JACKS**
All CCTP jacks shall be RJ45 style (Belden 110 CCTP Jack) using the four pair T568B wiring scheme with CCTP Central Control Pin Assignments.
- **FACEPLATES**
All faceplate connections shall use the Belden 110 style CCTP, eight position data jacks.
- Furnish and install dust covers/blanks in all CCTP jacks.
- Identify all items of equipment installed on the project. Each faceplate cover when applicable, all cable ends, and patch panels shall be labeled with the cable type, Security Component number, as per MCS Security, and wire distribution rack, using a Kroy Dura. Type 200 label marker or approved equal. Patch panels shall be marked to identify them as security.
- Properly identify all wire distribution racks with black plastic plates with 1/4" white engraved lettering on the face of each, permanently attached with two tapped screws. Example: MDF, IDF#1...
- Each port in the sixteen-port patch panel shall be labeled to match the camera cable numbers.
- Example of Security Component labeling at MDF:
Camera #1-MDF or Motion#1 – MDF etc...
Camera #1-MDF or Motion#1 etc...Camera #2-MDF or Motion#2 –MDF
- Example of Security Component labeling at IDF's:
Camera #1-IDF? or Motion#1 – IDF#? etc...
Camera #1-IDF? or Motion#1 – IDF#? etc...Camera #2-IDF#? or Motion#2 – IDF#?
- **SECURITY CABLE TESTING**
The contractor shall test all cables using one of these three Fluke meters, model 4000, 4100, or 4300 and then submit performance verification in soft copy format to MCS Information Technology Department. All UTP cables shall meet performance guidelines for Cat.6 cable and the MCS Information Technology standard of more than 3 db headroom on cables. This includes CCTP CAT.6 cable.

- **SECURITY CABLE INSTALLER / TESTER CERTIFICATION**
Cabling contractor shall submit to MCS proof that each cable installer and person testing cables has successfully completed training classes recognized by Building Industry Consulting Service International (BICSI) for installing and testing Unshielded Twisted Pair (UTP) Cat.6 cable and/or Uridium Manufacturer Certification, CCTP Manufacturer Certification, and all other certification requirements necessary to warranty all Security Equipment.

Electrical Outlets

Many dangerous situations exist due to the overuse/misuse of power strips and extension cords. These devices should be used only if absolutely necessary, and they should never be connected to each other in a “chaining” fashion. This is not only hazardous for students and employees but also dangerous for expensive computing equipment. Any such situations at your site must be rectified immediately. All computer and electronic equipment must be plugged into an Information Technology approved surge-protected outlet. In addition, outlets installed in floors are dangerous due to water spillage. Personnel should be asked to exercise caution when cleaning floors, watering plants, or performing other activities that might risk getting liquid or other foreign material in an electrical outlet.

Wireless Technology

Wireless computing is a convenient and relatively inexpensive way of connecting to a network. There are two distinct disadvantages. First, performance of wireless at this time is much inferior to an actual cable connection. For dynamic environments where a short-term, casual network connection is desired, this may not be a factor. However, for situations where a shared server will be used or a moderate to heavy load is expected, wireless performance will not be satisfactory. **Moderate or heavy load consists of but is not limited to video conferencing, video streaming, and file download exceeding 5MB.** The second disadvantage of wireless is related to the security risk that is inherent in wireless communications. A Request for Support, MCS 028, must be completed with the latest electronic form found in the Support Request Lotus Notes database BEFORE implementation of any wireless solution.

For situations where wireless is deemed appropriate, the Access Point must be the Cisco Aironet for both PC and APPLE configurations due to its ability to handle both environments and its stronger security and management functionality.

Video Conferencing

Video Conferencing allows individuals to meet and share information using video/audio equipment (cameras, microphones, etc.). Sessions **MUST BE SCHEDULED** at least two (2) weeks in advance. Request for desktop video conferencing must be submitted to the Department of Information Technology using a Request for Support, MCS 028, electronic form found in the Support Request Lotus Notes database.

Video/Audio Streaming

Video/Audio Streaming allows video and audio to be distributed at the desktop level. However, for situations where a shared server will be used or a moderate to heavy load is expected, wireless performance will not be satisfactory. The minimum system requirements to receive video/audio streaming are:

800 Mhz Processor
128MB Memory
20 GB Hard Drive
Windows 2000 or XP Professional Operating System (**must have current service pack**)
Internet Explorer v6.0with 128 encryption
DirectX v9.0

Several media players are available for video/audio streaming. The following media players are recommended:

Windows Media Player v9.0 or above (**must be installed**)
Quicktime v6.0 or above
RealPlayer v9.0 or above

Switch Equipment

10/100 3Com mini switch

- 3Com Office Connect Dual Speed Switch 8 Plus
3Com Part Number: 3C16791-US
Description: Unmanaged 8-port 10/100 switch
- 3Com Office Connect Dual Speed Switch 5 Plus
3Com Part Number: 3C16790-US
Description: Unmanaged 5-port 10/100 switch

"Mini-switches" are the current devices offering quick and inexpensive ways of providing increased connectivity. Although these devices solve some of the problems experienced in the past with switch equipment, their use must still be controlled because they hamper centralized management and facilitate the creation and use of computer labs, which are not recommended as methods of integrating technology into instructional curriculum. The remainder of this section outlines the restrictions for the use of switch equipment and situations where their use may be allowed.

The Department of Information Technology must approve the use of switch technology before it can be connected to the MCS network. Many classrooms had to disconnect a computer to enable the connection of a telephone; and, in these situations, Information Technology has approved the use of a switch. In all other situations, switches are considered a temporary solution for inadequate drops in a classroom and will be approved ONLY if all existing drops in the school are being used and a Request for Support, MCS 028, must be completed with the latest electronic form found in the Support Request Lotus Notes database. The appropriate number of network drops and the school's funding code must be included. No more than one (1) switch will be approved per classroom.

The MCS standard mini-switch is the 3Com office connect dual speed switch (see part numbers above). As mentioned previously, requests for use of a mini-switch may be made via a Request for Support, MCS 028, form found in the Support Request Lotus Notes database.

Switches approved for use by Information Technology may be used only in the authorized location and in the authorized manner. In addition, there can be no more than one (1) switch per room, and it must be the MCS standard switch. All nonstandard switches should be disconnected from the network immediately with the exception of those used in the 21st Century classrooms, which have recently been converted from token-ring to Ethernet using a 3Com 4-port Ethernet switch with an uplink port. This is nonstandard, but agreement was made previously to “grandfather” this particular piece of equipment.

Labs needing more than the standard six (6) drops installed via E-rate funds are not to be set up dependent on the use of switch equipment. A Request for Support, MCS 028, must be completed with the latest electronic form found in the Support Request Lotus Notes database, should there be a need for designed assistance for the additional network drops. Future applications such as video on demand and video conferencing will make the full port bandwidth necessary for desired performance. Those labs currently using hubs as the basis for their network connections must discontinue use of any nonstandard hubs. A Request for Support, MCS 028, must be completed with the latest electronic form found in the Support Request Lotus Notes database requesting that additional drops be installed or requesting approval to acquire and use the standard switch. [Note that the standard allows only one (1) switch per room so this may mean a reduction in the number of active workstations in the lab.]

Workstations

Specific configuration, (model and spec.), recommendations must be determined at time of purchase. Always refer to the MCS Purchasing website (http://www.mcsk12.net/aboutmcs_procurement_services_computers.asp) for purchases of approved hardware configurations. Contact the MCS Support Center, 416-2700, if you need assistance.

Network Connectivity – Hardware

Ethernet Network

	Network Adapter: 10/100 3Com PCI Adapter (PC Systems) Apple Built-in 10/100 Ethernet Adapter (Apple Systems) PC Integrated 10/100 Ethernet Adapter
Notebook PC Card Adapter	10/100 Intel or 3Com PC Card Adapter (Ethernet)
Network Printer Adapter:	Hewlett Packard JetDirect Adapter (Ethernet)
Cable System:	Cat.6 Giga Speed
Patch Cable:	Cat.6 Giga Speed
Switch:	Cisco SNMP Manageable Switch

Network Connectivity –Wireless

Access Point

- Cisco Aironet 350 Series (PN# AIR-AP352E2R-A-K9) 849
- Cisco Aironet 1200 Series (PN#AIR-AP1220B-A-K9) 999
- Cisco Aironet 1100 Series (AIR-AP1131AG-A-K9)

Wireless Card

- PC Built-in Adapter
- Cisco Wireless Adapter
- APPLE Built-in Adapter
- 3Com Wireless 11a/b/g PCI Adapter (Only when authorized by IT)

Point-Of-Service

Point-Of-Service:	PC Family (256MB RAM Min) PC Color Display
Network Adapter:	10/100 3Com PCI Adapter PC Integrated 10/100 Ethernet Adapter
Patch Cable:	Cat.6 Giga Speed
Other:	MMF Industries EDC232 Microcomputer Cash Drawer PC ASCII Terminal 3151, 3153, or WYSE-60 CAFS Custom Keyboard Scan 10 Keypad
Printer:	Epson Family w/Cable

SIS Hardware

Printer:	HP 8150N LaserJet
----------	-------------------

Miscellaneous Hardware

Removable Drive:	gb Flash Drive
CD Burner:	CDRW Drive and DVD

Software

The software supported by the District is listed below. It is recommended that the latest version of each application be used. Updated versions of some applications may require operating system and hardware updates.

Careers and Technology

Data Processing/Computer Programming:

Microsoft Visual InterDev V6 Microsoft C++ Visual Basic 6.0	Microsoft Access
---	------------------

Standard Software for School and Administrative Offices

Type	PC Application	APPLE Application
Mainframe Communication	PC Personal Communication 3270	DataComet
Database	Microsoft Access	File Maker Pro
Network Operating System	Windows 2003 Server Windows 2000 Server Windows 2000 Advanced Server	Apple OSX Server
Virus Protection	Computer Associates ITM	Virex
Desktop Publishing	Microsoft Publisher	Microsoft Publisher iWorks
Spreadsheet	Microsoft Excel	Microsoft Excel, Numbers
Word Processing	Microsoft Word	Microsoft Word, Pages
Presentation	Microsoft PowerPoint	Microsoft PowerPoint, Keynote
Integrated	Microsoft Office	Microsoft Office
Library Automation	Atrium, Book Systems, Inc	Atrium, Book Systems, Inc
Point of Service (Cafeteria)	Linux, CAFS Software, In-house API Programs and Associated files, Pcomm 3270	N/A
Internet Browser	Microsoft Internet Explorer, Firefox, Safari	Microsoft Internet Explorer, Firefox, Safari
E-mail	Lotus Notes	Lotus Notes
Conferencing	Microsoft Net Meeting	N/A
Website: http://sms.mcsk12.net/ChancerySMS		N/A

Standard Software for Instructional Workstations

Type	Win Application	MAC Application
Desktop Operating System	Microsoft Windows 2000/XP/Pro	MAC OS
Network Operating System	Microsoft Windows 2000 Server Microsoft Windows 2003 Server	Apple Share Server OS 9 Mac OS X Server
Virus Protection	CA Integrated Threat Mgmt	CA Integrated Threat Mgmt
Security	FoolProof for all non-WIN 2000/XP machines. (Windows 2000 and above have built-in security). DeepFreeze Pro	FoolProof for MAC (MAC OS-X and above have built-in security).
Utility Tools	Symantec Suite	Symantec Suite
Word Processing	Microsoft Office Word Pages	Microsoft Office Word Pages
Spreadsheet	Microsoft Office Excel Numbers	Microsoft Office Excel Numbers
Database	Microsoft Office Access	Apple works/Filemaker Pro Microsoft Office Access
Presentation	Microsoft Office PowerPoint Keynote	Microsoft Office PowerPoint Keynote
Multimedia	Hyper studio	Hyper studio iMovie iPhoto, iLife
Web page Design	Dreamweaver Contribute PhotoShop Elements Learning Village Homepage Designer	Dreamweaver Contribute Learning Village Homepage Designer
Internet Browser	Microsoft Internet Explorer, Firefox, Safari	Microsoft Internet Explorer, Firefox, Safari
E-mail for Teachers	Lotus Notes Ten-Nash account, iNotes	Web Access Ten-Nash account, iNotes
Lesson Planning	Riverdeep Learning Village	Riverdeep Learning Village

District Reviewed Instructional Software/Web Resources

(Note: The following is not an inclusive list. For more information contact International Society for Technology in Education: <http://www.iste.org> – **The school is required to purchase and maintain a contract with the vendor for installation, training, and support of District Reviewed Software.**)

Type	Grade Level	Application	Platform
Encyclopedia	K-12	Grolier's Multimedia Encyclopedia	MAC, WIN, Internet
		Encarta	WIN
Website: http://www.itstimetoread.org	K-12	Web resource to support literacy instruction	MAC or WIN
Web search educational engine	K-12	NetTrekker	MAC, WIN
Digital video streaming website	K-12	Discovery Streaming	MAC, WIN
Intervention Program designed to help bottom quartile students. Program begins at the 1.5 reading level (first half of first grade)	3-8	Scholastic's Read 180	MAC or WIN
Beginning-reading software that blends	K-2	Scholastic's Wiggleworks	APPLE or WIN
Activities to develop pre-reading skills	PreK-2	Bailey's Book House	MAC or WIN
Testing resource to manage and assess reading and math progress (NOT INSTRUCTIONAL PROGRAM)	K-12	Renaissance Learning Products (Accelerated Reader, Accelerated Math, Early Literacy, etc.)	MAC or WIN
Spreadsheet	K-8	The Cruncher	MAC or WIN
Graphing software	Pre-K-5	The Graph Club	MAC or WIN
Concept mapping	PreK-3	Kidspiration	MAC or WIN
Concept mapping	K-12	Inspiration	MAC or WIN
Create Timeline to order events	K-8	Timeliner	MAC or WIN
Create maps	K-8	Neighborhood Map Machine	MAC or WIN
Mapping software	12-Sep	Geographical Information Systems (GIS)	Mac or WIN Website below for Mac: (http://www.gueritte.plus.com/geomax.html)

Storytelling tool allowing students to create electronic books.	K-8	Imagination Express	MAC or WIN
Slideshow presentations, paint, draw, write	K-8	Kid Pix Studio Deluxe	MAC or WIN
Write and illustrate stories	PreK-5	Kid Works Deluxe	MAC or WIN
Multimedia hypertext authoring software	K-12	Hyperstudio	MAC or WIN
Activities encourage students to develop higher-level thinking skills.	Pre-K-8	Thinkin' Things	MAC or WIN
Mathematics instructional support	6-12	Riverdeep Destination Math	Web Based and WIN
Reading instructional support	K-3	Riverdeep Destination Reading	Web Based and WIN
Reading instructional support	K-3	Compass Learning Odyssey Reading	Web Based and WIN
Course Recovery	6-12	Plato Learning	Web Based and WIN

Telephones (VOICE OVER ATM)

System Assistance/Request for Support

The following guidelines are for approved and funded projects only. All telephones, hardware, and software must be installed to meet MCS guidelines. For assistance with new or modified networked systems and major technology planning, a Request for Support, MCS-028, must be completed with the latest electronic form found in the Support Request Lotus Notes database. The completed requests may be prioritized by Executive Staff. A site visit from the staff of Information Technology may be made to assist with:

- Explanations of technical concepts, as needed
- Training needs
- Equipment and installation requests
- Security Authorization Requests
- Cost estimates

Installation

Advantages of the current system include phones in classrooms, 5-digit dialing district-wide, consistent performance even during peak periods such as student registration, and features such as

voice mail and auto attendant. The emergency calling capability has been reviewed and approved by the police, fire, and 911 emergency departments. Whenever a 911 call is made, automatic notification goes to MCS Security with information giving the location of the caller.

A current list of school phone numbers is located at:
http://www.mcsk12.net/school_search.asp?menuItem=ALL.

Support

The voice system runs over the same ATM fiber network as our data. Thus, the ongoing monitoring, management, and support done for data extends also to the phone system. All problems or questions must be reported through the MCS Support Center, 416-2700. Technicians will be dispatched by the MCS Support Center as needed.

MAC is an acronym for the words Move, Add, Change. Customer requests that require:

- moving something that already exists,
- adding something new to a service that already exists, or
- changing an existing service.

All MAC's require the submission of a Request for Support, MCS 028, electronic form found in the Support Request Lotus Notes database. Requirements will be gathered and a price quotation provided for the principal's/director's review and funding approval.

Appendix A

**OFFICE OF STUDENT INFORMATION
SMS SCHOOLS
SECURITY AUTHORIZATION FORM**

SECURITY AUTHORIZATION – USERID REQUEST

Userids are assigned by Data Security. The principal or manager must sign the bottom of this form. **Please bring the signed copy to training.** This form will be forwarded by the training instructor to the Office of Student Information then to Data Center Services after training has been completed.

Name of Requestor: _____

Department Name: _____

Job Title: _____

Location: _____ Phone Number: _____ Date SMS Training Completed: _____

ID Type: Temporary _____ Permanent _____

Effective Date: _____ End Date: _____ (if temporary)

TYPE OF ACCESS: (select only one)
(see pg. 2 for explanation)

School Admin _____ School Health _____ HR Compliance _____

School Secretary _____ District Health _____ Pupil Services Ctr _____

School View _____ District View _____

APPROVAL:

Principal//Manager: _____ Date: _____

Training Instructor: _____ Date: _____

FOR STUDENT INFORMATION USE ONLY

Data Specialist: _____ Date: _____

FOR SECURITY ADMINISTRATOR USE ONLY

Date Received: _____ Date Completed: _____

Data Security Analyst: _____

School Admin Access Level

- Principals
- Assistant Principals
- SIA (Student Information Administrator)

Able to update: Students & Contacts
Schedules
Attendance
Grades
Enrollment
Behavior
Health
Teachers

School Secretary Access Level

- General Office Secretary

Able to update: Students & Contacts
Attendance
Grades
Enrollment
Behavior
Teachers

School View Access Level

- Librarian
- Technical Support
- Nurse
- Guidance Counselors
- Zone Directors
- Data Support

Able to view: Students & Contacts
Schedules
Attendance
Grades
Enrollment
Behavior
Teachers

Able to update: Health
(Nurses only)

District View Access Level

- District Offices
- Pupil Services Center
- Human Resources - Compliance

Able to view: Students & Contacts
Schedules
Attendance
Grades
Enrollment
Behavior
Teachers

Able to update: Teachers
(HR Compliance only)

Able to update: Behavior
(PSC only)

Notes

Training sessions can be accessed using the following URL:

Technology Training Center Website:

<http://www.mcsk12.net/admin/it/ttc/pdc.html>

*The Security Authorization Form must be signed by the principal or manager prior to training. **Please bring the signed copy to training.***

Please bring a copy of pertinent manuals and other documents to training sessions, which can be downloaded using the following URL:

Docushare

<http://docushare1/dscgi/ds.py/View/Collection-41>
or

Student Information Website

http://www.mcsk12.net/aboutmcs_student_information.asp

Chancery SMS can be accessed using the following URL:

Chancery SMS

<http://sms.mcsk12.net/ChancerySMS>

**Memphis City Schools
Office of Student Information
Room 314
Fax #416-5441
Email: sisd@mcsk12.net**

SECURITY AUTHORIZATION FORM

**SECURITY AUTHORIZATION – USER ID
REQUEST**

Userids are assigned by Data Security. Your principal or manager and resource steward must sign the bottom of this form and forward to Data Center Services, Room 250. Your principal or manager will be notified of userid and password.

Name of Requestor: _____

Department Name: _____

Location: _____ Phone Number: _____

ID Type: Temporary _____ Permanent _____

Effective Date: _____ End Date: _____ (if temporary)

(Attach Access Memo)

Resource: * TSO: _____ CYBORG: _____
* CICS: _____ COGNOS BI: _____
DB2: _____ EP: _____
INFOR/WALKER: _____ *** MCSK12 DOMAIN: _____

Change Control – (Application Services Only): _____

* = Attach Form MCS-0037

*** = Attach Form MCS-0036

Approval:

Principal/Manager: _____ Date: _____

Resource Steward: _____ Date: _____

Approved: Disapproved:

FOR SECURITY ADMINISTRATOR USE ONLY

Date Received: _____ Date Completed: _____

Data Security Analyst: _____
(Signature)

MCS0035 Revised 7/11/08

Memphis City Schools SCHOOL-LEVEL SECURITY FORM

USERIDS are added and deleted by Data Security. The requestor's principal must sign the bottom of this form and forward to Data Security Administrator, Data Center Services, Room 250. If added, the requestor will be notified of userid and password. Please have each requestor fill out a form.

School Name: _____ Location Code: _____

School Phone Number: _____

Name of Requestor: _____ Add Delete

Job Title of Requestor: _____

Responsible for Chancery Grade-Out: Yes

SAA Secretary: Yes

Warehouse Requisitions (T11137) Yes

School Textbooks (K72 / Walker) Yes

Comments: _____

Security Authorization: My signature below indicates I understand and agree to the following:

Password: Passwords and user codes are unique to me, and I will not share or give to others for their use. I am responsible for my password and will not use an easily guessed password, such as my name, initials, or spouse's name.

Non-Disclosure Clause:

I understand that I am requesting access to confidential data and that I will not divulge any information to any person or organization without written permission from an authorized representative of Memphis City Schools. I also understand that any copies, printed forms, handwritten documents, diskettes, or other data storage are to be treated in the same confidential manner.

I am aware that failure to comply with the above statements is cause for disciplinary action, including but not limited to, immediate termination of employment and may result in civil liability.

SIGNATURE OF REQUESTOR / TITLE

DATE

SIGNATURE OF PRINCIPAL

DATE

***** **FOR DATA SECURITY USE ONLY** *****

Date Received: _____ Date Completed: _____

Data Security Analyst: _____

Approved: Disapproved: Reason: _____

MCS-0036 07/11/08

Memphis City Schools

SECURITY AUTHORIZATION DATA ACCESS FORM

Name of Requestor: _____

Department/Division Name: _____

Phone Number: _____ Location: _____

TYPE OF ACCESS

(Read)	(Update)	FILE NAME and/or TRANSACTIONS
<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____

Non-Disclosure Clause: I understand that I am requesting access to confidential data and that I will not divulge any information to any person or organization without proper authorization. I also understand that any copies, printed forms, handwritten documents, or diskettes of the same confidential data will be treated in the same manner. I am aware that failure to comply with this statement is cause for disciplinary action.

_____ SIGNATURE OF REQUESTOR/TITLE	_____ DATE
_____ SIGNATURE OF SUPERVISOR/TITLE	_____ DATE
_____ SIGNATURE OF DATA STEWARD/TITLE	_____ DATE

FOR SECURITY ADMINISTRATOR USE ONLY

Date Received: _____ Date Completed: _____

Data Security Analyst: _____

(Signature)

Approved: Disapproved:

Reason: (if not approved)

Memphis City Schools

NONSTANDARD PURCHASE FORM

Complete this form and return to the Department of Information Technology, Room 250, Administration Building.

Name: _____ **Date:** _____

Location: _____ **Req. No.:** _____

Requested hardware/software configuration:

Intended use:

Justification for deviation from system standard:

I understand that the hardware/software configuration listed above is nonstandard. I agree to assume full responsibility for technical support and maintenance.

Signature: _____ **Date:** _____

MCS-0047
07/11/2008

Procurement Services

Service/Material/Equipment Justification

Form # 92153

(SUBMIT THIS FORM WITH REQUISITION FOR LINE ITEMS OF \$5,000.00 OR MORE)

PLEASE ATTACH RATIONALE FOR ANY EXPENDITURE IN EXCESS OF \$50,000.00. PLEASE INCLUDE THE LONG-RANGE BENEFITS AND THE SPECIFIC STRATEGIC GOAL(S) THIS EXPENDITURE WILL SUPPORT.

Division _____ Department/School _____

Requisition Number _____ Funding: Fund _____ Proj _____ Function _____ Obj _____

Funding Description _____

(General Funds, C.I.P., Grants, School Allocation, Federal, School Activities, Nutrition, etc.)

Product Description (Detailed, attach appropriate documentation) _____

Program Description Summary (Detailed, attach appropriate documentation) _____

Vendor _____ (If bids were taken by your location, you must submit all supporting documentation for this justification. **Please list all vendors contacted as well as the prices submitted. If a single source vendor was selected or a vendor other than the low bidder, please justify the decision on a separate sheet.**) Please indicate in the space provided below, if applicable, the minority classification(s) for the vendor(s), i.e., B=Black, W=Woman, H=Hispanic, AA=Asian American, AI=American Indian, AN=Alaskan Native, or O=Other (define) in the space provided below.

Vendor #1 _____ Price \$ _____ Minority Classification(s) _____

Vendor #2 _____ Price \$ _____ Minority Classification(s) _____

Vendor #3 _____ Price \$ _____ Minority Classification(s) _____

School Sites Involved _____

Number of Students Served _____ Grade/Subject Target Area _____

Signature _____ Date _____

White Copy - Requisition

Yellow Copy - School

WHZD#17-02/92153

**Request Form
Lotus Domino Web Access**

All new teachers including (Exceptional Children, ESL, and Librarians) to the Memphis City Schools **must** fill out a request form for Lotus Domino Web Access. **Lotus Domino Web Access** will be your electronic communication tool within the Memphis City Schools system. Complete this request form and FAX it to 416-0114.

Domino Web Access training is **not** required for teachers. If you desire training, on-line registration is available at <http://www.mcsk12.net/admin/it/ttc/pdccatalog.html>, or complete this registration form indicating workshop, date, and time. FAX it to 416-4185 OR mail it to: Technology Training Center, 3772 Jackson Avenue, Memphis, TN 38108.

Date: _____

Please print

Last Name: _____

First Name: _____

Middle Initial: _____
(Middle initial must be given if available; if not, please indicate NONE)

Job Title: _____

Supervisor Name/Title: _____

School/Dept Name: _____ RM# _____

Loc. Code: _____ Mail Route: _____

Daytime Phone: _____

Home/Alternate Phone: _____

FAX#: _____

List workshop ID code, date, and title

WKSHP ID	DATE	TIME	CLASS TITLE
WAC	_____	_____	Lotus Web Access

ACCESS CONTROL AT SCHOOL SITES

Any access to the MCS network must be approved by the principal based on MCS instructional and/or administrative policies, regulations, and guidelines.

For Internet and e-mail access, an Acceptable Use Agreement must be signed by the user and kept on file at his/her site. Access will be terminated promptly when an employee leaves the MCS system or violates the Agreement.

All files, Internet use, and e-mails are subject to review at any time by MCS.

Principal's Signature: _____ Date: _____

**MCS0053
07/11/08**

VPN Access Record

Name _____

Division or Company Name: _____

Phone # _____ E-mail Address: _____

Network Services Needed (Mainframe, Notes, SMS, etc.):

Special Notes:

Access Start Date: _____

Access End Date: _____

Username Assigned: _____

Group Assignment: Base\MCS_____

Special Settings or Restrictions:

Signature: _____ Date: _____
Requestor

Approved: _____ Date: _____
Principal / Director / Project Manager

Approved: _____ Date: _____
Executive Director of Information Technology

Record Created by: _____ Date: _____

MCS-0054
7/11/2008

**Send this completed package to
Information Technology (Room 250)
for
Review/Approval
School Information**

Date _____ School Name _____ Loc Code _____

Requisitioner _____ Phone () _____ E-mail _____

About the Vendor(s)

Company Name _____ Phone () _____

1. What is the instructional purpose for this purchase?

2. Is this instructional technology purchase consistent with the District Technology Plan and your School Improvement Plan (SIP)? Yes No

3. How will you implement and support this classroom technology?

5. Is an instructional server required? Yes No
If yes, which platform? Apple PC Other

6. Are additional data and electrical drops required? Yes No
(If yes, please complete and attach MCS-028 to request drops and electrical.)

7. Are you ordering a MCS-approved standard switch? Yes No NA

NOTE: Standard Switch: 10/100 3Com Mini-switch – Part No. 3C16791-US (8 ports) or 3C16790-US (5 ports)
[One switch per room is allowed for temporary connectivity with the authorization of Information Technology.
An attached (Appendix A, MCS-028) form must contain the school's budgetary coding and the principal's approval for installation of the required drops.]

8. Is wireless technology being purchased? Yes No

NOTE: Vendors must implement wireless technology according to MCS Technology Guidelines and Procedures.
(Only cart configurations for wireless will be approved.)

9. Is instructional software being ordered? Yes No

If yes, list software and continue: _____

10. Has vendor verified that school hardware meets the minimum requirements to run the software? Yes No

11. Has technical support for software been purchased? Yes No

NOTE: It is required that ongoing technical support be purchased, maintained, and funded by the school.
Example: Expert Support Plan (ESP+) for Renaissance Learning Products

12. Is standard software included in the order? Yes No

MCS Standard software should be purchased for all instructional workstations including **Microsoft Office and Anti-Virus Protection**.

Below is a list of additional forms that MAY be required with this form:

- Request for Support Form MCS-028
(Request for wiring, cabling, mini-hubs/switches, wireless, and special support)
- NonStandard Purchase Form
(Justification for deviation from system standard)
- PROCUREMENT SERVICES/SERVICE MATERIAL EQUIPMENT JUSTIFICATION Form (Submit with requisition for line item network, wiring, and cabling of \$5000.00 or more.)

Approved: Information Technology _____ Date _____

MCS-0055
07/11/08

Appendix B

**PROCEDURES REGARDING THE RECEIPT, INVENTORY, TRANSFER, AND
REPAIR OF EQUIPMENT
in the
MEMPHIS CITY SCHOOLS SYSTEM**

Definition: Equipment can be defined as any item (excluding furniture) that has a value in excess of \$100.00, or items that are identified by the Director, Division of Procurement Services, and as such becomes part of the equipment inventory system.

I. Principals and/or Division Heads Responsibility as Trustee

- A. The responsibility and accountability of equipment at a location will rest with the principal at the school level, or the division head when no school is involved.**
- B. The Division of Procurement Services will supply the Inventory Control office with a copy of the purchase order or other documentation on all equipment purchased with Board of Education funds. When any equipment is purchased with school funds, booster club funds, or is donated and has not been properly marked and inventoried, the principal will notify, in writing, the Division of Inventory Control and Warehousing. Each site will assume responsibility of marking and recording this equipment, which automatically becomes the property of Memphis City Schools.**

II. Issue and Storage of Equipment

- A. Equipment should be located in an area which will facilitate maximum utilization. The principal or the division head will establish and maintain a system that will ensure proper accountability at all times.**
- B. Every effort will be made to control and protect equipment from theft and vandalism. Storage areas should be utilized which will offer the maximum security. The Division of Security should be contacted if adequate security is not available to protect equipment assigned to location.**

III. Repair of all Equipment

- A. Any non-microcomputer equipment that is found to be inoperative or damaged will be reported to the Division of Maintenance (320-6250) so that it may be properly repaired.**
- B. Form No. 14671 (Equipment Transfer Form) will be completed on equipment in need of repair. One copy is to be attached to the equipment and the other copy retained on file in the office until the equipment is repaired. The driver picking up the equipment will sign the school copy to indicate the date it was picked up for repair. (One form for each item of equipment.).**
- C. Equipment that cannot be repaired will be removed from the school's inventory. This report (Form No. 14671) will be submitted by the Division of Maintenance. A copy of the form will be returned to the school or division. If this equipment is from a special funding source, the appropriate supervisor is to be contacted by the Inventory Control office for disposal.**
- D. Principals or division heads having items not normally repaired by the Division of Maintenance, but found to be in an un-repairable condition, shall report such to the Inventory Control office on Form No. 14671. Equipment to be disposed of will be picked up by the Inventory Control office for disposal. (All items may be listed on one form.) Please see separate page entitled Equipment Transfer Form.**

- E. Vocational and cafeteria equipment in need of repair, which is normally repaired by the Division of Maintenance, will be referred by the appropriate division to the Division of Maintenance for service.

IV. Transferring and Loaning of Equipment

- A. The transfer of equipment between locations will not be done without approval of the appropriate principal or division head. The transfer of special funded equipment will also be coordinated with the division concerned. **Form No. 14671 will be filled out in triplicate on any equipment being transferred.** One copy should be forwarded to the Inventory Control Office, 1300 Farmville; one copy will be retained by the school losing the equipment; and one copy will be sent to the receiving location.
- B. **Equipment will not be sold or traded by the principal or the division head without proper administrative approval.**
- C. The principal or division head will be responsible for any equipment on loan to their activity. Equipment, which will be on loan for thirty (30) days or longer, will be transferred using Form No. 14671 and listed on the equipment inventory of the receiving location.
- D. Procedures regarding removing equipment by school/office personnel on a temporary basis: Occasionally equipment assigned to a school location inventory may need to be taken home by teachers or administrative personnel. The principal or department head, having full responsibility and accountability for all equipment to that location, will approve or deny the removal of any equipment.

If approved, an agreement of responsibility for replacement/repair should be signed by the person removing the equipment. This agreement, which may be in letter or memo form, should show the following information:

- quantity and description
- serial number
- Memphis City Schools identification number
- date of removal
- name, address, and telephone number of person removing the equipment
- specific language stating that the signee, who is removing the property, will be responsible for repair or full replacement in the event of any theft or damage to the equipment

The principal or department head and the party removing the equipment will both sign and date this agreement. Each should retain a copy. The original of the agreement will be sent to Inventory Control and a copy will be sent to the Division of Security Services.

Upon the return of the property to the school or administration location, individual copies shall be noted with the return information, including date returned and the condition upon return, and signed by the principal or the department head as receiving the property.

Copies of this return paperwork shall be forwarded to Inventory Control and the Division of Security Services in order to clear individual liability.

V. Procedures for Disposal/Pick up of Equipment

- A. When you identify equipment in need of disposal or transfer, complete an Equipment Transfer Form with the following information: quantity, description including model#, brand/manufacturer, disposition (DISPOSAL or TRANSFER), serial number, MCS ID Tag#, and comments (REMOVE FROM INVENTORY or TRANSFER TO ____ ELEM.)

- B. Forward the white and yellow copies of the Equipment Transfer Form to the Division of Inventory Control and Warehousing (Loc. 153).**
- C. Retain the pink copy of the Equipment Transfer Form for your records.**
- D. Be sure to place the equipment to be picked up in a centralized location.**

VI. Annual Inventory of Equipment

- A. An annual inventory of all equipment will be accomplished prior to the end of school year using the Location Equipment Inventory Record Report. This report is distributed annually in early January to each location and returned to Inventory Control by the date indicated in the cover letter.**
- B. All missing items will be reported immediately to the Inventory Control office on Form No. 14671 outlining all circumstances (i.e., date reported missing, last date seen, serial number, etc.).**
- C. Any equipment not located on the inventory report will be listed on Form No. 14671 and sent to Inventory Control. Action will be taken to add these items to the equipment inventory. All school inventories will be forwarded to Inventory Control, 1300 Farmville. Form 14671 should be signed and dated by the principal or authorized delegate.**

VII. Missing or Stolen Equipment

- A. When equipment is stolen, immediately notify Security Services at 416-5773 and the Memphis Police Department to file reports. There is no reimbursement for stolen equipment without a timely report.**
- B. Within one (1) day of the acknowledgement of the theft, complete an Equipment Transfer Form with the following information: quantity, description including model# and brand/manufacturer, disposition (STOLEN), serial number, MCS ID Tag#, and comments.**
- C. A Break-in, Theft & Damage Report must be completed and submitted to the Office of Security within one (1) day of the acknowledgement of the theft.**
- D. Forward the white and yellow copies of the Equipment Transfer Form, a copy of the MCS Break-in, Theft & Damage Report, and the MPD theft report to the Division of Inventory Control and Warehousing (Loc. 153).**
- E. Forward the MCS Break-in, Theft & Damage Report, and MPD theft report to the Division of Security.**
- F. Retain the pink copy of the Equipment Transfer Form, a copy of the MCS Break-in, Theft & Damage Report, and the MPD theft report for your records.**

IMPORTANT NOTE: There will no longer be a category for Missing Equipment. If the equipment is in your building, you must have staff locate the item. If the piece of equipment cannot be located, please follow the procedures above for stolen items.

Appendix C

**PROCEDURES REGARDING THE
REPAIR OF COMPUTER EQUIPMENT IN THE
MEMPHIS CITY SCHOOLS SYSTEM**

A. Any standard computer equipment that is found to be inoperative or damaged requires a ticket request in order for a timely repair to occur. (website: hd.mcsk12.net/tiweb).

B. The on-site technician will create a ticket in Track-it for any computer equipment that needs to leave the premises for repair. This ticket will include the serial#, model, MCS#, room#, and customer's name.

C. Computer equipment that cannot be repaired should be removed from the site's inventory. This report (Form No. 14671 - Equipment Transfer Form) must be submitted to Inventory Control by the site. School Technical Specialist (STS) must certify that the hard drive has been re-formatted for security purposes. STS must sign the Equipment Transfer Form to indicate that the data has been removed.

A copy of the form will be returned to the school or division. If this equipment is from a special funding source, the appropriate supervisor is to be contacted by the Inventory Control office for disposal (Example: Exceptional Children).

D. Problems related to inoperative large-screen TV/Monitors connected to a computer should be reported to the MCS Support Center (416-2700). All other TV's should be reported to Facility Support (320-6307) by the school designee. A School Technical Specialist will perform the initial diagnosis and determine the next course of action. Information Technology Customer Support must submit all requests for service on non-warranty TV/Monitors to MCS Facility Repair. Please note that MCS Facility Repair will not accept a request for service on any problem that is computer related. The user is responsible for contacting the vendor to schedule any repair needed on warranted TV/Monitors.

Appendix D

BOARD POLICY

ACCESS TO TELECOMMUNICATIONS NETWORKS #1115

Adopted 9/19/96

I. PURPOSE

To promote educational excellence, equity, efficiency, and communications through the appropriate use of telecommunications and other technologies that have transformed the ways that information may be accessed and communicated.

II. SCOPE

This policy applies to all students, employees, board members, contractors, vendors, and guests. Guests include parents, volunteers, and any other persons or agencies authorized to use or have access to Memphis City Schools (MCS) telecommunications equipment.

III. POLICY STATEMENT

Effective use of telecommunications, electronic information sources, and networked services is critical in preparing students for jobs and life in the 21st century; in facilitating business dealings among employees and board members and between employees or board members and the public; and in communicating with parents and other concerned citizens about the welfare of students. Technological literacy will enable students and teachers to explore and communicate with thousands of libraries, databases and experts from many fields/areas. It will also enable employees and board members to complete business transactions in a more efficient and timely manner. Finally, technological literacy will enable parents to keep abreast of their children's progress and assignments as well as communicate with teachers and administrative personnel about their children's well being.

MCS supports the use of electronic communications systems and expects that staff will thoroughly integrate the electronic use of voice, data, and video throughout the curriculum and the school system. MCS also expects that staff will provide guidance and instruction to students, employees, board members, contractors, vendors, and guests in the appropriate use of such resources.

In accordance with federal law, MCS shall ensure the Internet safety of students through enforcement of acceptable use guidelines, and by the operation of technology protection measures. The acceptable use guidelines include prohibitions on access to inappropriate material; monitoring Internet and e-mail traffic to prevent access to inappropriate material; restrictions on access to students' personal information; and prohibitions on "hacking" and other unauthorized access. The technology protection measures include computer software programs or "filters," with respect to all Internet-enabled computers, that will block access to visual depictions that are obscene, that contain child pornography, or (with respect to use of the computers by minors) that are harmful to minors.

MCS reserves the right to review, monitor, and restrict at any time information stored on or transmitted via MCS-owned or leased equipment and to investigate inappropriate use of resources. Correspondence in the form of electronic mail may be a public record under the State of Tennessee's public records law and may be subject to public inspection.

Use of MCS telecommunications and electronic information sources network will be permitted upon submission and approval of agreement forms by students, employees, vendors, contractors, and guests. Network use is intended for educational and professional purposes. Any other use may be

considered inappropriate use of MCS resources. All network use by students that is unrelated to or inconsistent with educational development is unacceptable. All users of the MCS network must demonstrate responsible behavior in compliance with this policy at all times.

All employees are expected to conduct their use of these systems with the same integrity as in face-to-face or telephonic business operations. Violations of the terms and conditions stated in the agreement may result in disciplinary action. Any use perceived to be illegal, harassing, offensive, in violation of other Board policies, or that reflects adversely on the school district can be the basis for disciplinary action up to and including termination.

The Superintendent shall develop and implement procedures to provide guidance for students, employees, vendors, contractors, and guests in the appropriate and ethical use of telecommunications such as the Internet.

IV. RESPONSIBILITY

A. The Superintendent is responsible for ensuring that appropriate administrative rules and regulations are developed to implement this Policy.

B. Principals are responsible for ensuring that school personnel are trained and have appropriate authorization to access MCS telecommunications networks, and for reviewing and approving all information published by their schools.

C. Executive staff is responsible for ensuring that all employees, vendors, contractors, and guests within their jurisdiction are trained and have appropriate authorization to access the telecommunication networks, and for reviewing and approving all information published by their departments.

D. Teachers are responsible for ensuring that students are trained to use the district's telecommunication networks. Teachers are responsible for monitoring use of the Internet in their classrooms.

E. Users of the district's telecommunication networks, including contractors, consultants, and parents, are responsible for complying with the provisions of this policy, the pertinent administrative rules and regulations, and the acceptable use policy agreement.

F. Any questions concerning this policy, the pertinent administrative rules and regulations, or the acceptable use policy agreement should be directed to the Department of Fiscal Services.

G. The Board of Commissioners is responsible for ensuring that board members comply with the pertinent provisions of this policy.

H. The Division of Internal Audits is responsible for determining if this policy is followed.

V. REFERENCES

Children's Internet Protection Act, 2 U.S.C. §7001

Electronic Communications Privacy Act, 18 U.S.C. §2510

Copyright Act of 1976, 17 U.S.C. §101

Electronic Mail Communications Systems, T.C.A. 10-7-512

Computer Offenses, T.C.A. 39-14-601 et seq.

Access to Telecommunications Networks - Administrative Rules and Regulations 1115

Network Publishing - Administrative Rules and Regulations 1115.1

Conflict of Interest - Policy 4504

Moonlighting/Outside Employment - Policy 4508

Student Behavior - Policy 5151.2

**ADMINISTRATIVE RULES AND REGULATIONS
ACCESS TO TELECOMMUNICATIONS NETWORKS #1115**

COORDINATION

The Department of Information Technology is responsible for managing the MCS network and for providing technical assistance to district personnel on use of MCS computers and on compliance with applicable policies, regulations, and guidelines. The "MCS network" is the system of computers, terminals, and databases connected by telecommunication lines owned or leased by the Memphis City Schools District, including the hardware, software, and other technology attached or connected to, installed in, or otherwise used in connection with the system.

ACCESS CONTROL AT SCHOOL SITES

Any access to the MCS network must be approved by the principal based on MCS instructional and/or administrative policies, regulations, and guidelines.

For Internet and e-mail access, an Acceptable Use Agreement ("Agreement") must be signed by each user and the parent/guardian of students and kept on file at the school. Access will be terminated promptly when an employee or student leaves the MCS system or violates the Agreement.

All files, Internet use, and e-mails are subject to review at any time by MCS or by the school.

ACCESS CONTROL AT ADMINISTRATIVE SITES

Any access to the MCS networks must be approved by the appropriate executive staff member based on MCS instructional and/or administrative policies, regulations, and guidelines.

For Internet and e-mail access, an Acceptable Use Agreement ("Agreement") must be signed by each user and kept on file in the executive staff member's office. Access will be terminated promptly when an employee leaves the MCS system or violates the Agreement.

All files, Internet use, and e-mails are subject to MCS review at any time.

MCS NETWORK RULES - STUDENTS

Students will be allowed to use e-mail at school only for educational purposes. Parents must give written consent prior to such use. Teachers and instructional personnel will periodically monitor students' online communications.

Students who receive e-mail messages or attachments that are obscene, vulgar, harassing, threatening, or that incite hatred toward any group must report the correspondence to their teachers. Students must also report any materials that make them feel uncomfortable.

Students shall not transmit personally identifiable or personal contact information about themselves or others, except the student's e-mail address, without prior consent by the parent and the teacher. Personally identifiable or personal contact information shall include name, address, telephone

number, photograph, social security number, school name, and classroom.

School websites cannot include pictures or names of students without prior written consent of the parents and teacher. All other personally identifiable information (e.g., address and phone number) is strictly prohibited on a website.

MCS NETWORK RULES - ALL USERS

All users, including students, employees, parents, contractors, and any other person accessing the MCS network, shall comply with the following rules:

The MCS network may be used only for educational and professional purposes consistent with MCS's goals. Commercial use (advertisements, business logos, etc.) of the MCS network is prohibited, unless specifically permitted in writing by the Department of Communications. A list of school adopters is permitted.

-Users will only use MCS-approved e-mail applications.

-Users cannot use the Internet to access information that is obscene or vulgar, that advocates dangerous or illegal acts, or that advocates violence or hatred toward any group. Written approval by the teacher and the parent is required when a research project involves accessing information on the Internet relating to dangerous or illegal acts or violence or hatred toward a group.

-Materials that are offensive, threatening, or that otherwise are intended to harass or demean recipients must not be transmitted, including jokes that are intended to offend, harass, or intimidate.

-Files, data, or information of others must not be improperly accessed or misused.

-Plagiarizing is prohibited. Plagiarism means to steal and pass off the ideas or words of another as one's own. Users cannot use another's ideas or words without crediting the author.

-Copyright infringement is a violation of federal law. Users should be aware that most of what is on the Internet is protected by copyright. Copyrighted materials include, but are not limited to, writings, articles, web pages, designs, music, videos, and software. The illegal installation, use, or transmission of copyrighted materials is prohibited.

-Websites cannot display photographs or videos of employees or individuals not affiliated with MCS without the individual's prior consent, unless the individual is an historic figure or a public figure.

The following activities and uses of the MCS network are prohibited:

-Downloading, installing, and using of programs that infiltrate computing systems and/or damage software components, including "viruses" and "worms."

-Downloading, installing, and using of any program or software without prior written authorization of the Department of Information Technology.

-Intentionally disrupting network traffic, crashing the network, or gaining unauthorized access to the files of another user.

-Using inappropriate language in any type of communication on the MCS network. Inappropriate language includes, but is not limited to, language that is vulgar, profane, abusive, and threatening.

- Using the MCS network to personally attack, harass, or threaten another person or intentionally or recklessly publishing false information about another person.
- Private or illegal use of the MCS network. Incidental personal use by employees during lunch and break times is permitted.
- Using the MCS network for political lobbying.
- Anonymous communications.
- Mass e-mailing of unsolicited or unwanted messages ("spamming"), including text, software, video images, graphics.
- Playing computer games, unless part of an educational program.
- Falsifying, concealing, or misrepresenting the user's e-mail identity ("spoofing").
- Forwarding messages without the knowledge and permission of the original user, except in circumstances in which forwarding is customary or expected.
- Downloading music and sound recordings without prior approval.
- Any action which violates existing Board policy, local, state, or federal law.

SECURITY

Users shall comply with all MCS network security requirements and shall not attempt to bypass such requirements in any way or compromise the security of data by spreading computer viruses or vandalizing data, software, or equipment.

Authorized users will be provided with an MCS network account; each user must use a password to access the account. Users are personally responsible at all times for the proper use of the account.

Leaving personal account, password, or any other access information stored on any school computer is prohibited.

Sharing MCS network accounts and passwords with anyone is prohibited. User accounts must not be left open and unattended.

Backup copies of documents are the responsibility of the user.

Precautions to prevent viruses are the responsibility of the user.

Messages must be deleted or archived regularly to conserve space. MCS reserves the right to delete or archive messages at any time.

User passwords must be changed regularly using combinations of letters and numbers, avoiding standard English words and names.

Unauthorized access, including "hacking," is prohibited.

Security violations must be reported to the principal/appropriate executive staff member immediately.

REMOTE ACCESS

Remote access is access to the MCS network from any non-school location, such as home or public libraries.

If MCS provides remote access to students, parents/guardians are exclusively responsible for monitoring their children's remote use, including all e-mail traffic and Internet activity.

Parents or employees who have been granted remote access to the MCS network are the only appropriate users of the network. They are prohibited from sharing their password with anyone else, and are responsible for any consequences from inappropriate sharing of the password. If a child gains access and subsequent violations or other improper actions occur, the parent will be held accountable for the actions.

Any external access to the MCS network, including high-speed connections (e.g., cable modems, DSL, analog, or wireless) is prohibited without approval in writing from the Department of Information Technology.

Remote access directly to a school or office local area network (LAN), or stand-alone personal computer (PC) using software such as Apple Remote Access (ARA), PC Anywhere or Carbon Copy, is prohibited unless approved in writing by the Department of Information Technology. Audits will be conducted periodically to detect the presence of software, which allows remote access. Anyone having unapproved software of this nature installed on MCS equipment will be subject to disciplinary action.

CONTRACTORS AND CONSULTANTS

Contractors and consultants shall be governed by the same policy and rules and regulations as employees of MCS. Additional restrictions may be imposed when access is given to confidential information.

REPORTING ALLEGED POLICY VIOLATIONS

Alleged student violations shall be reported to the teacher. The teacher or other staff person shall report the alleged violation to the principal. The principal shall investigate the alleged violation, with appropriate input from the Department of Information Technology. If a violation exists, the principal will impose appropriate sanctions.

Alleged teacher violations shall be reported to the principal. The principal shall investigate the alleged violation, with appropriate input from the Department of Information Technology. If a violation exists, the principal shall impose appropriate sanctions.

Alleged violations by employees other than those affiliated with schools or by contractors or consultants shall be reported to the appropriate division director or Executive staff member. If a violation exists, the division director or executive staff member shall impose appropriate sanctions.

Alleged violations by Board members shall be reported to the president of the Board for appropriate investigation and, if necessary, imposition of sanctions.

Alleged violations of policy discovered by the Department of Information Technology shall be reported to the principal or to the appropriate senior management official.

Alleged violations of policy by parents/guardians should be reported to the Department of Information Technology. If a violation exists, appropriate sanctions shall be imposed.

Principals, division directors, and executive staff members shall report all violations of the Access to Telecommunications Networks Policy and Regulations to the Department of Information Technology's Security Administrator.

MCS may revoke Internet and e-mail access in its sole discretion. If a student's access is revoked, MCS will continue to provide the student with a meaningful educational program.

SANCTIONS

Violations of these rules and regulations or the accompanying Agreement may result in loss of access to the MCS network. Additional disciplinary action may also be taken, including suspension/expulsion for students and termination of employment for employees. When applicable, law enforcement agencies may be involved.

USER AGREEMENT

The attached Acceptable Use Agreement ("Agreement") must be read and signed by the user and parent/guardian of students and placed on file at the school prior to access to the MCS network. Students and parents must sign a new Agreement at each school the child attends at the time of registration. Employees must sign an Agreement at the time of employment.

ADMINISTRATIVE RULES AND REGULATIONS NETWORK PUBLISHING #1115.1

Opportunities for MCS students and employees to publish documents electronically fall into two major categories - the Internet and the Intranet. Although many procedural issues related to the publishing of electronic documents are similar to those that govern traditional publishing, others are new. This document outlines the responsibilities of potential MCS publishers and provides guidelines for the publishing of home pages and other electronic documents in both environments.

INTERNET

The Internet is a worldwide system of networks, which makes a vast quantity of information and resources available to anyone who has a computer, a modem, and an Internet access account. Examples of documents, which MCS might publish on the Internet, include job vacancies, school assignment information, bus routes, student project information, and other information of public interest.

INTRANET

The Intranet is the MCS internal network, which can be used to provide information of interest to employees. Examples of internal communications include district, student, and administrative applications.

POTENTIAL MCS PUBLISHERS

Potential electronic publishers include all students and employees of MCS. General publishing rules apply to both groups and are detailed below. Procedural manuals for publications that are specific to particular groups of publishers or types of documents may be desirable to provide additional guidelines. As such manuals are developed, they must be reviewed by the Department of Information Technology prior to distribution.

GENERAL PUBLISHING RULES

Content published through the MCS network (both the Internet and Intranet) must comply with the following regulations:

-All publications must comply with all policies and regulations of MCS (including the MCS network acceptable use guidelines) and all state, federal, and international laws concerning copyright, trademarks, intellectual property, and use of computers. Copyright infringement is a violation of federal law. Users should be aware that most of what is on the Internet is protected by copyright. Copyrighted materials include, but are not limited to, writings, articles, web pages, designs, music, videos, and software. The illegal installation, use, or transmission of copyrighted materials is prohibited.

-Publications must include a statement of copyright or a trademark when appropriate, and indicate that permission has been secured to include copyrighted or trademark materials. All use of trademarks, names, text, graphics, and other items owned by others must be reviewed and approved in writing by the principal or division/department director (or delegate). Devices must be reviewed by the principal or division/department director (or delegate) for compliance with copyright, trademark, and related laws.

-The Division of Library Services shall provide guidance on review and approval of copyrighted or trademark materials.

-All websites shall contain "Terms of Use" provisions approved by the Department of Information Technology. In addition, websites shall contain privacy notifications, where deemed appropriate by the Department of Information Technology.

-All MCS publications must reside on the MCS network. Any exceptions must be approved by the Department of Information Technology.

-All content must be appropriate, decent, in good taste, and not intended to harass or demean individuals or groups.

-Correct grammar and spelling should be used.

-Factual information must be documentable.

- Publications must identify affiliation with MCS and have the official MCS logo on the title page.
- The title page of all publications must provide a link to the MCS home page. Publications cannot include any other link without prior written approval by the Department of Information Technology.
- The date last updated is required on all publications.
- All publications must include the e-mail address of the person maintaining the page.
- The title page of all publications must include the statement, "Memphis City Schools does not discriminate in its programs or employment on the basis of race, color, religion, national origin, handicap/disability, sex, or age. For more information, please contact the Office of Equity Compliance at (901) 416-6670."
- Commercial use (advertisements, business logos, etc.) is prohibited, unless specifically approved in writing by the Department of Communications. A listing of school adopters is permitted.
- Documents should be high quality and structured for clarity and readability.
- Websites cannot display photographs or videos of employees or individuals not affiliated with MCS without the individual's prior consent, unless the individual is an historic figure or a public figure.
- All publications must be reviewed and approved as described below.

NETWORK PUBLISHING BY DISTRICT ADMINISTRATIVE PERSONNEL

Design and Development:

Design of the district's website is the responsibility of the Department of Communications. Other websites intended for the public may be designed and developed by individuals or groups of employees with permission of appropriate management staff. All web pages linked from the MCS district website are subject to monitoring by the Department of Communications.

Approval and Publication:

Information published on the Internet by MCS district administrative personnel that states or suggests district-wide position or policy must be approved by the Department of Communications. In addition, any links from the district home page must be approved by the Department of Communications. Publications that pertain to subject matter or content in a specific division must be approved by the division director or appropriate executive staff member.

Internet publication involves tying the new information via links to existing networked information. The Web Page Specialist in the Department of Communications is responsible for final testing and linking all new Internet information published at the district level. New publications should be submitted to the Department of Communications.

All websites shall contain the following provision: "Any links or frames connecting to sites other than MCS website and schools websites are for reference only and MCS and the school do not endorse or approve the sites or their content."

Maintenance:

Management staff of the site/division originating the publication is responsible for ensuring that content is accurate and current. This includes the regular review, testing, and modification of all links and the withdrawal of any documents, which become inaccurate or irrelevant.

NETWORK PUBLISHING BY SCHOOL PERSONNEL AND STUDENTS

Design and Development:

Project pages and other documents for publication may be designed and developed as desired by individual students, teachers, or groups, as appropriate. The content of the school's home page is left to the discretion of the school except for the required elements specified in the General Publishing Rules section of this document.

School websites cannot include pictures or names of students without prior consent of the parents and the teacher. All other personally identifiable information (e.g., address and phone number) is strictly prohibited on a website.

Approval and Publication:

The school's home page must be reviewed by the Department of Communications. All other documents published by schools must be reviewed and approved by the school principal before being published on the Internet.

The school principal is responsible for implementation of documents on the appropriate school or project server. The principal is also responsible for maintaining a backup of the information so that a prompt recovery can be made in the event of corruption or loss.

An e-mail should be sent to inform the Web Page Specialist in the Department of Communications when a document is published on a school or project server if a link from a district-level page is desired.

The school principal shall appoint a Web Page Monitor to oversee the school's official web page and to ensure that all material published by the school follows all policies, regulations and guidelines. The Web Page Monitor shall report all improprieties to the school principal. The school shall provide the Department of Communications with the name of the monitor.

Maintenance and Disclaimer:

School principals are responsible for ensuring that all publications implemented by their respective schools are updated as necessary to maintain accurate and current content. This includes the regular review, testing, and modification of all links and the withdrawal of any documents, which become inaccurate or irrelevant.

THE WEBMASTER

The Web Page Specialist in the Department of Communications shall provide assistance as requested in the design and development of electronic documents. In addition, the Web Page Specialist shall monitor all MCS electronic publications.

In general, documents developed by district students, teachers, and administrative personnel will reside on a district server (at the central office) and will be interlinked with documents from all divisions/areas within MCS. The Webmaster in the Department of Information Technology is responsible for maintaining the integrity and recoverability of the district Internet and Intranet servers. Therefore, documents intended for publishing on a district server must be formatted using standard language approved by the Webmaster in the Department of Information Technology.

MEMPHIS CITY SCHOOLS

E-mail and Internet Acceptable Use Agreement

I. INTRODUCTION

1. MCS is pleased to be able to offer access to the MCS network for electronic mail (“e-mail”) and the Internet. To gain access to e-mail and the Internet, all students must obtain parental permission and must sign and return the attached Student Access Release and Authorization Form to the school office. Employees must sign and return the attached Employee Access Release and Authorization Form to the appropriate executive staff member or school principal.
2. The “MCS network” is the system of computers, terminals, and databases connected by telecommunication lines owned or leased by the Memphis City School District, including the hardware, software, and other technology attached or connected to, installed in, or otherwise used in connection with the system.
3. While our intent is to make Internet access available to further educational and professional goals and objectives, students and employees may find ways to access other materials as well, including offensive, illegal, and dangerous materials. By signing below, students and parents acknowledge that MCS cannot entirely prevent such access, and accept sole responsibility for the consequences of such access. We believe that the benefits from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any possible disadvantages. Ultimately, parents and guardians are responsible for setting and conveying the guidelines that their children should follow on the use of the Internet just as they do on the use of all media information sources such as television, telephones, movies, and radio.
4. This educational opportunity also entails a certain amount of responsibility. It is important that employees, students, and parents/guardians read carefully and understand this Acceptable Use Agreement (“Agreement”).
5. When access to the Internet is granted, it is extremely important that the rules in this Agreement be followed. Violations could result in temporary or permanent loss of access to the Internet. Violations may also result in disciplinary action, including suspension/expulsion for students and termination of employment for employees. When applicable, law enforcement agencies may be involved.
6. MCS has the right to restrict or terminate any user’s access to the MCS network at any time and for any reason.

II. REVIEW AND MONITORING BY MCS

1. MCS reserves the right to review, monitor, and restrict at any time information stored on or transmitted via THE MCS NETWORK and to investigate suspected inappropriate use of resources.

2. MCS will monitor and read e-mail communications. **USERS SHOULD HAVE NO EXPECTATION OF PRIVACY IN E-MAIL TRANSMITTED, RECEIVED, AND STORED ON AND THROUGH THE MCS NETWORK.** Users **SHOULD** not use MCS network e-mail to transmit or discuss any confidential matters.
3. Correspondence in the form of electronic mail may be a public record under the state of Tennessee's public records law and may be subject to public inspection.
4. MCS may monitor or review users' Internet activity at any time. Users should have no expectations of privacy in their Internet traffic and activities.

III. STUDENT RESPONSIBILITIES

1. Students are responsible for good behavior on the MCS network just as they are in a classroom or a school hallway. Communications on the MCS network are often public in nature. General school rules for behavior and communications apply. Appropriate MCS personnel will determine whether behavior and communications are appropriate, and those determinations will be final.
2. The MCS network is provided for students to conduct research and communicate with others for educational purposes. Access to network services is provided to students who agree to act in a considerate and responsible manner. A student's signature and parent/guardian permission are required. Access is a privilege, not a right, and entails responsibility.
3. Individual users of the MCS network are responsible for their behavior and communications over the network. It is presumed that users will comply with district guidelines and will honor the Agreement they and their parents/guardians have signed.
4. During school, teachers will help guide students toward appropriate materials. Outside school, families bear responsibility for guidance on the Internet just as they do with information sources such as television, telephones, movies, radio, and other potentially offensive media.

IV. EMPLOYEE RESPONSIBILITIES

1. Use of the MCS network is a privilege, not a right, and inappropriate use may result in cancellation of that privilege.
2. Appropriate executive staff members or school principals will deem what is inappropriate use, and that decision is final. Employees who are granted access must remember that they represent MCS and as such, must respect the rights of others, protect the integrity of the information technology, and observe all relevant laws, regulations, and contracts including software licensing agreements and copyright laws.

V. MCS NETWORK RULES

A. MCS Network Rules - Students

1. Students will be allowed to use e-mail at school only for educational purposes. Parents must give written consent prior to such use. Teachers and instructional personnel have the authority to review a student's e-mail and e-mail attachments.
2. Students who receive e-mail messages or attachments that are obscene, vulgar, harassing, threatening, or that incite hatred toward any group must report the correspondence to their teachers. Students must also report any materials that make them feel uncomfortable.
3. Students shall not transmit personally identifiable or personal contact information about themselves or others, except the user's e-mail address, without prior consent by the parent and the teacher. Personally identifiable or personal contact information includes name, address, telephone number, photograph, social security number, school name, and classroom.
4. School websites cannot include pictures or names of students without prior consent of the parents and teacher. All other personally identifiable information (e.g., address and phone number) is strictly prohibited on a website.

B. MCS Network Rules – All Users

(a) All users, including students, employees, parents, contractors, and any other person accessing the MCS network, shall comply with the following rules:

1. The MCS network may be used only for educational and professional purposes consistent with MCS's goals. Commercial use (advertisements, business logos, etc.) of the MCS network is prohibited, unless specifically permitted in writing by the Department of Communications. A list of school adopters is permitted.
2. Users will only use MCS approved e-mail applications.
3. Materials that are obscene, offensive, threatening, or that otherwise are intended to harass or demean recipients must not be transmitted, including jokes that are intended to offend, harass, or intimidate.
4. Users may not use the Internet to access information that is obscene or vulgar, that advocates dangerous or illegal acts, or that advocates violence or hatred toward any group. Written approval by the teacher and the parent/guardian is required when a student research project involves accessing information on the Internet relating to dangerous or illegal acts or to violence or hatred toward a group.
5. Personal employee information must be given out only in an instructional context or in the performance of MCS business.
6. Files, data, or information of others must not be improperly accessed or misused.

7. Plagiarizing is prohibited. Plagiarism means to steal and pass off the ideas or words of another as one's own. Users cannot use another's ideas or words without crediting the author.
8. Copyright infringement is a violation of federal law. Users should be aware that most of what is on the Internet is protected by copyright. Copyright materials include, but are not limited to, writings, articles, web pages, designs, music, videos, and software. The illegal installation, use, or transmission of copyrighted materials is prohibited.
9. Websites cannot display photographs or videos of employees or individuals not affiliated with MCS without the individual's prior consent, unless the individual is an historic figure or a public figure.

(b) The following activities and uses of MCS network are prohibited:

1. Downloading, installing, or using of programs that infiltrate computing systems and/or damage software components, including "viruses" and "worms."
2. Downloading, installing, or using of any program or software without prior written authorization of the Department of Information Technology.
3. Intentionally disrupting network traffic, crashing the network, or gaining unauthorized access to the files of another user.
4. Using inappropriate language in any type of communication on the MCS network. Inappropriate language includes, but is not limited to, language that is vulgar, profane, abusive, and threatening.
5. Using the MCS network to personally attack, harass, or threaten another person or intentionally or recklessly publish false information about another person.
6. Private or illegal use of the MCS network. Incidental personal use by employees during lunch and break times is permitted.
7. Use of the MCS network for political lobbying.
8. Anonymous communications.
9. Mass e-mailing of unsolicited or unwanted messages ("spamming"), including text, software, video images, graphics.
10. Playing computer games, unless part of an educational program.
11. Falsifying, concealing, or misrepresenting the user's e-mail identity ("spoofing").
12. Forwarding messages without the knowledge and permission of the original user, except in circumstances in which forwarding is customary or expected.

13. Downloading music and sound recordings without prior approval.
14. Any action, which violates existing Board policy, local, state, or federal law.

C. Network Publishing

In order to be approved for publication on MCS or school web pages, all materials must comply with the Administrative Network Publishing Rules and Regulations. Copies of the Network Publishing Rules are available at the school.

D. Security

1. Users shall comply with all network security requirements and shall not attempt to bypass such requirements in any way, compromise the security of data, or vandalize data, software, or equipment.
2. Authorized users will be provided with a MCS network account; each user must use a password to access the account. Users are personally responsible at all time for the proper use of the account.
3. Leaving MCS network account, password, or any other access information stored on any school computer is prohibited.
4. Sharing MCS network accounts and passwords with anyone is prohibited. User accounts must not be left open and unattended.
5. Backup copies of documents are the responsibility of the user.
6. Precautions to prevent viruses on MCS equipment are the responsibility of the user.
7. Messages must be deleted or archived regularly to conserve space. MCS reserves the right to delete or archive messages at any time.
8. User passwords must be changed regularly using combinations of letters and numbers, avoiding standard English words and names.
9. Security violations must be reported to the principal/appropriate executive staff member immediately.

E. Remote Access

1. Remote access is access to the MCS network from any non-school location, such as home or public libraries.
2. If MCS provides remote access, parents/guardians are exclusively responsible for monitoring their children's remote use, including all e-mail traffic and Internet activity.

3. Parents or employees who have been granted remote access to the MCS network are the only appropriate users of the network. They are prohibited from sharing their password with anyone else, and are responsible for any consequences from inappropriate sharing of the password. If a child gains access and subsequent violations or other improper actions occur, the parent will be held accountable for the actions.
4. Any external access to the MCS network, including high speed connections (e.g., cable modems, DSL, analog, or wireless) is prohibited without approval in writing from the Department of Information Technology.
5. Remote access directly to a school or office local area network (LAN), or stand-alone personal computer (PC) using software such as Apple Remote Access (ARA), PC Anywhere or Carbon Copy, is prohibited unless approved in writing by the Department of Information Technology. Audits will be conducted periodically to detect the presence of software, which allows remote access. Anyone having unapproved software of this nature installed on MCS equipment will be subject to disciplinary action.

VI. DISCLAIMER OF LIABILITY

1. MCS makes no warranties of any kind, either express or implied, that the functions or the services provided by, or through, the MCS network will be error-free or without defect. MCS will not be responsible for any damage users may suffer including, but not limited to, loss of data or interruption of services.
2. MCS is not responsible for the accuracy or quality of information obtained through or stored on the MCS network. MCS will not be responsible for the content of any advice or information received by a user from a source outside MCS, or any costs incurred as a result of such advice. MCS will make reasonable efforts to supervise students' Internet and e-mail use but will not be responsible for claims and liabilities arising out of such use.
3. MCS will not be responsible for financial obligations incurred or arising through the use of the system.
4. MCS is not responsible for the communications of individuals utilizing the network.
5. MCS does not assume any responsibility for the content of material published on school web pages.
6. Parents will be held financially responsible for any harm to the system as a result of the student's intentional misuse.

Note: The STUDENT ACCESS RELEASE AND AUTHORIZATION FORM may be ordered from the MCS warehouse as form No. 14196

(Return this portion to the School Principal.)

MEMPHIS CITY SCHOOLS
Student Access Release and Authorization Form

As a condition of using the MCS network, I agree to comply with the E-mail and Internet Acceptable Use Agreement (“Agreement”). I have read and I understand the Agreement. Should I commit any violation, my access privileges may be revoked and disciplinary action may be taken, including suspension/expulsion.

I UNDERSTAND THAT MY MCS NETWORK ACCOUNT IS NOT PRIVATE. I CONSENT TO MCS MONITORING ALL MY ACTIVITY ON THE NETWORK, INCLUDING E-MAIL, INTERNET ACTIVITY, AND ALL FILES AND DOCUMENTS STORED IN THE MCS NETWORK.

Student Signature: _____

As the parent or legal guardian of the student signing above, I grant permission for him/her to access networked computer services such as e-mail and the Internet. I understand that he/she is expected to use good judgment and follow rules and guidelines in making contact on the MCS network, including the rules and guidelines set forth in the Acceptable Use Agreement (“Agreement”). MCS cannot be responsible for the student’s use of the MCS network, including any ideas and concepts that he/she may gain by his/her use of the Internet or for the actions he/she takes through use of the Internet. I release MCS, the School, their officers, agents, and employees from all costs, claims, and liability resulting from use of the MCS network by the student.

I have read the Agreement and accept the rules and conditions in the Agreement. I release MCS, the School, their officers, employees, and agents from any claim arising out of the student’s use of the MCS network. I agree to indemnify and to hold harmless MCS, the School, their officers, employees, and agents from any costs, liability, or claims arising from the student’s use of the MCS network.

Parent/Guardian Signature: _____ Date: _____

Student Name: _____

School: _____ Grade: _____

Student’s Soc. Sec. #: _____ Birth Date: _____

Home Address & Zip Code: _____

Home Phone: _____ Work Phone (if applicable): _____

Note: The EMPLOYEE ACCESS RELEASE AND AUTHORIZATION FORM may be ordered from the MCS warehouse as form No. 14197

(Return this portion to the Executive staff member or Principal.)

MEMPHIS CITY SCHOOLS
Employee Access Release and Authorization Form

As a condition of using the MCS network, I agree to comply with the E-mail and Internet Acceptable Use Agreement (“Agreement”). I understand that access to MCS network, including e-mail and Internet capability, is a privilege and agree to the following:

1. I will abide by the rules adopted by MCS including the rules in the Agreement.
2. **I UNDERSTAND THAT MY MCS NETWORK ACCOUNT IS NOT PRIVATE. I AGREE THAT MCS MAY REVIEW AND MONITOR AT ANY TIME ALL INTERNET USE AND ANY E-MAIL OR OTHER MATERIAL STORED ON ANY SYSTEM PROVIDED BY MCS AND MAY EDIT OR REMOVE ANY MATERIAL. I** waive any right, which I may otherwise have in and to such material.
3. I understand that the MCS network is to be used only in pursuit of MCS goals.
4. I release MCS and its officers, employees, and agents from any claims and damages arising from my use of the MCS network.

I have read and understand the Agreement. I understand that any violation of the Agreement is unethical, potentially illegal, and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and disciplinary action may be taken, including termination of employment.

I agree to indemnify and to hold harmless MCS, the School, their officers, employees, and agents from any costs, liability, or claims arising from my use of the MCS network.

Employee’s Name (Please print) _____
Location

Employee’s Signature _____
Date

APPROVED:

Principal’s Signature _____
Date

Executive Staff Member Signature _____
Date

Appendix E

COPYRIGHT NOTICE

It is required that the following information be posted in prominent locations throughout the school site.

**MANY COMPUTER PROGRAMS ARE PROTECTED BY COPYRIGHT. 17
U.S.C.\S\101. UNAUTHORIZED COPYING IS PROHIBITED BY LAW AND
PUNISHABLE BY FINE, IMPRISONMENT, OR BOTH.**

Appendix F

TELEPHONE DEPLOYMENT GUIDELINES

(Handset Models Mapped to MCS Employees Categories)

Telematrix 2105 (2 lines, caller id, speaker):

- Principal
- Director and above
- Executive Secretary
- Receptionist

Telematrix 1105 (1 line, caller id, speaker):

- Assistant Principal
- Coordinator
- Administrator
- Manager

Telematrix 1104 (1 line, speaker):

- Conference/Meeting Room
- Staff requiring a speakerphone

Telematrix 1103 (1 line):

- All other employees requiring a phone

Telematrix 1101 (1 line, base model):

- Classrooms
- Required customer access phones
(Ex: Hall phone at Avery)
- Teachers Lounge