TECHNOLOGY BEST PRACTICES

LOGGING IN TO THE NETWORK ON YOUR WORKSTATION:

You will receive your username/password from your school administrator.

The first time you log in to your machine, you will be prompted to set a more secure password. If you wish to create a new password in the future, hit Ctrl-Alt-Delete, then click the "Change password…" button.

DISTRICT WEBSITE/STAFF PORTALS

The Madison Public Schools website can be accessed at www.madison.k12.ct.us. Here you will find a Staff link (www.madison.k12.ct.us/staffportals) to directories and commonly used teacher portals, such as Webmail, Finalsite, Infinite Campus, AESOP, SchoolDude, and teacher resources and instructions. Elementary teachers login at www.madison.k12.ct.us/admin MS & HS teachers login by clicking Community Login on any of our webpages.

RETRIEVING EMAIL

Your e-mail address: yourusername@madison.k12.ct.us

From work, access e-mail through Microsoft Outlook.

From home, you can access e-mail by going to https://owa.madisonct.org/school (also found on the MPS website under Staff>Portals). To log in, use "campus\" at the start of your username, i.e. "campus\wardb". Use the same password you use to log in to the network on your workstation.

SEEKING HELP

The Technology Department has posted an abundance of online resources featuring answers to some frequently asked questions and video tutorials for various district software applications. K-4 teachers can access a Technology Resource Portal from their desktops or by going to Staff>Portals on the district website (teacher resource password = mpstech). Grades 5-12 teachers will find technology resources when they log in to the Finalsite, and click on the Teacher Resources tab. If you can't find the answers to your questions from these resources, feel free to contact the appropriate members of the Tech Department directly:

Integrating instructional technology into your lesson plans and software application support:

Gr K-6: Michael Ginsburg at ginsburgm@madisonk12.ct.us

Gr 7 -12: Michael Kiefer at kieferm@madison.k12.ct.us

Web page and software application support

Webmaster: Rita Boland at bolandr@madison.k12.ct.us

For hardware and network issues, each building is serviced by a technology paraprofessional. Here are some of the issues they address:

Connecting to the Internet

Equipment set-up

Hardware issues

Mobile laptop cart usage

Network/connectivity issues

Passwords

Printer/Printing

Program installation

Software updates

SMART Board troubleshooting

To request help from a tech para, you will need to log into **SchoolDude**, which has its own icon on your desktop, or through the staff portal. Please be aware that the first time you login you will receive a message that you are not in the system. At that point create your account by following the attached login instructions.

Tech Paraprofessional	**Location**	**email**
Elizabeth Clyde	All Elementary Schools	clydee@madison.k12.ct.us
Hugo Ordonez	Polson Middle School	ordonezh@madison.k12.ct.us
Wendy Ruiz	Brown Middle School	ruizw@madison.k12.ct.us
Jake Siciliano	Daniel Hand High School	sicilianoj@madison.k12.ct.us

BOARD POLICIES

Best Practice: Be certain to read and understand all Board of Education Policies regarding the use of technology in the District.

Discussion:

Technology policies may be found on the District website (http://madison.k12.ct.us) under the Board of Education drop-down menu item. Specifically, policies 4140, 4141 and 4150 in the Personnel section refer to employee use of technology.

PASSWORDS/SECURITY

Best Practice: Change your password often.

Discussion: Changing your password is one of the simplest things you can do to prevent unauthorized use of your network account. To change your password you must be logged-on. Once you are logged-on with your current (old) password, use the three key combination Ctrl-Alt-Del and one of the choices will be “change password…”

You will be prompted to enter your old password and then to enter your new password twice. The reason you must enter the new password twice is that the screen will not display the password as you type it. Entering it twice will improve the likelihood that you typed it correctly.

Choosing a strong password is important. A strong password is at least six (6) characters long and contains a mix of letters and numbers. If possible, use a mix of upper and lower case with the letters. Passwords are case sensitive and must be typed exactly the same way they were defined.

A network administrator cannot display your password but can change it. Should you forget your password, contact the Technology Department.

Best Practice: Never share your password with anyone and never log on using someone else’s account.

Discussion: Sharing your password means that someone else can log on to your computer pretending to be you. Even if you trust the individual completely, it means that you are responsible for anything done while they are logged on as you. Any e-mails sent will be coming from your account and will appear as though you sent them. Any website visited will be logged to your account.

Inappropriate use of the network will be attributed to the user logged on at the time of such use, regardless of whether anyone else may have known that person’s password.

Using someone else's user id to log into a computer is equivalent to impersonating someone else and is a fraudulent use of that person’s account. This is a very serious violation of both district policy and the law.

Best Practice: Never allow a student to use a teacher workstation.

Discussion: Teacher workstations are physically and logically connected to many more resources than are student computers. Allowing a student physical access to your workstation opens up a great deal more possibilities and opportunities for network intrusion.

Teacher workstations in general have access to our student information system and other administrative software applications. If you allow a student to use your PC and you are signed on, that student will have access to read and send e-mail from your account, read and modify sensitive student data including grade information, and depending upon your job responsibilities, IEP information, evaluation information, the contents of your H: drives, and so forth.

Allowing a student to use your machine, especially if you are logged-in to the network is probably the worst security mistake you can make.

Best Practice: Never walk away from your workstation if you are logged-in. Always logoff or lock your workstation if it will be unattended for any reason.

Discussion: To logoff or lock your workstation, use the keystroke combination Ctrl-Alt-Del. “Lock your computer” and “logoff” are the first two choices. The advantage to locking your machine is that when you unlock it, you will be able to pick-up where you left-off. *Even faster, hit the Windows key + L to lock your workstation with a single stroke.*

If you intend to be away from your desk longer than a few minutes, you should logoff. That will close your software programs and release any data you may be reviewing on shared applications.

CONFIDENTIAL DATA

Best Practice: Never store student data (or sensitive data of any sort such as personnel information, social security numbers, etc) on a flash drive or a notebook computer. For that matter, the local hard drive of your desktop should not contain confidential information either. You should only store sensitive data on a network drive (not even the local C: drive of your desktop). Save all confidential data on the network's H: Drive. *See also E-MAIL USE below.*

Discussion: Flash drives or notebook computers are easily lost or stolen (flash drives especially). No data that could identify a student, or any personal information about a student, an employee, or yourself for that matter should ever be stored on portable equipment or media. Furthermore, a desktop's local hard drive is less secure than a remote network drive; therefore, all sensitive data should be stored on your H: Drive.

If your job requires frequent use of this type of information, refer to your building administration for further options. Depending on the application, certain functions are remotely accessible through encrypted, secure connections. These situations are rare for classroom teachers but from time to time come up.

SAVING YOUR FILES

Best Practice: Save everything to your home directory (H: drive).

Discussion: Your H: drive is a network shared drive reserved for your use. It can be found in *My Computer* and has your username associated with it. Only you and a network administrator can access your H: drive. The major reasons to use your H: drive instead of your local hard drive (C: drive) are that you can access your H: drive from any administrative computer in the District, and all the files on your H: drive are backed-up nightly. Saving to your C: drive is risky in that the files will not be backed-up. If your hard drive fails, you will lose all files stored there.

E-MAIL USE

Best Practice: Check your e-mail often.

Discussion: Checking your e-mail several times a day will keep you up-to-speed on important information your administrators and colleagues want to communicate to you. If, for example, your daily schedule needs to be altered in some way, e-mail is the least disruptive way for your colleagues to communicate this to you. In addition to the beginning and the end of the day, e-mail should be checked at least once during the day (between classes, during a planning period, etc.).

Best Practice: Subscribe to you building's and the district's e-Notify updates.

Discussion: This will keep you informed on any important building or district news by sending you automatic updates directly to your e-mail inbox. Sign up by going to the MPS district home page and selecting SUBSCRIBE.

Best Practice: Always use your district e-mail account for school business.

Discussion: All e-mail is subject to the same e-discovery, records retention, and Freedom of Information Act requirements as paper documents. As a result, it is very likely that some day, you may be asked to produce all of your business related e-mails regarding some specific issue. Using your personal e-mail account even once for correspondence regarding that issue could call into question all of your personal e-mail.

Additionally, all District e-mail is backed-up and archived and would be more readily available if necessary.

Best Practice: Consult with your building administrator regarding the practice in your building for corresponding with parents via e-mail.

Discussion: No discussion is required.

Best Practice: Never write anything in an e-mail that you would not be willing to say directly to anyone or that could possibly be interpreted as unprofessional.

Discussion: Anyone can forward an e-mail intentionally or unintentionally. Once you are in a list of addressees, anything can happen. There may be "BCC's" that you cannot see on the list of people who received the e-mail. If you reply or reply to all, you may be in for an unpleasant surprise. Keep all e-mail correspondence very professional.

Best Practice: Do not send any confidential information through e-mail.

Discussion: Once an e-mail message is sent over the internet, it travels unencrypted (in plain text) and can be read fairly easily by hackers attempting to steal identities and so forth. A discussion with your building administration should help clarify confidentiality concerns and best practices.

NIGHTLY RESTART

Best Practice: Be sure to <u>restart</u> your computer at the end of every day before you leave your classroom. You do not need to shut down. You do not need to wait for it to restart to finish.

Discussion: This will allow Microsoft updates to install on your computer in the least disruptive way.