Manhattan-Ogden Information Technology (IT) Basics

How do I get a district username and password?
-After an employee completes the necessary paperwork with Human Resources an account will be created. This process should be complete once district information has been processed. Once they are created the account information should be provided when staff leave the Human Resources department.

What should I do if I have a technology problem?
-The first step is to submit a Helpdesk ticket. Everyone with a district username and password can login to the School Dude Helpdesk program:
https://login.schooldude.com/sso/default.aspx?acctnum=992185344&productid=ITD
(this link should be on your desktop – check to see if you have it already). If you have a more immediate problem, please contact your building lead tech who can direct you to the support you need.

How do I set up a password in Outlook?
-Once you have a district username and password (these should have been provided when starting with the district) you can access your district e-mail. Your password in Outlook is the same as it is for logging into your computer.
If you wish to change your password see the Network Password Reset on the Informational Technology page of the district website.

*If in the user ID it says USERID@msad.usd383.org instead of USERID@usd383.org then call the Networking Office to update your account in the system. Once that is complete it can be changed to USERID@usd383.org it will connect and function fine.

How do I Access Webmail?
-Webmail allows employees who have their usernames and passwords to access their mail from any Internet connection. The address is: http://outlook.com/owa/usd383org.onmicrosoft.com or you can go to the Manhattan-Ogden website: http://www.usd383.org/ then click on District then Technology and click the Webmail link on the left side of the page.

How can I get greater access to the Internet to research classroom needs?
-Faculty and staff have the ability to gain greater access to the Internet than the students, so that they can do research for their classes and areas. Once the faculty or staff member has a district username and password (see getting a district account above) they can go to the site https://10.36.254.254:4100, you will see a warning page. Click on continue or I understand the risks. Next, type in their district username and password and make sure the Domain is MSAD.USD383.ORG then click login. At this point the faculty/staff member has more access out through the firewall to the Internet. Please remember that using district technology is meant for district related use only – please see district policy IIBG (at the end of this document) if you have other questions.

How do I get wireless connectivity for my district laptop?
- Turn on the laptop wait for the Microsoft screen to appear (then count to ten)

Hit Ctrl-Alt-Del and then a user entry screen should appear (if instead you see a button that says "other" click on it). At the user login screen be sure below the username and password entry it says it will try to log into USD383. Enter your district user name and password.

How do I install printers on my district computer/laptop?
-Please see the PDF document in the network drives T:\IT Documentation\Printers. This document will provide a step-by-step process on how to add printers.

Where to save documents?
-The IT department configures systems to save documents to their H:\ drive (see Drive Description below). The second option would be to an "external" location (also see below).

Describe the different drives (what they are used for).
-There are several "drives" on the computer/laptop. The IT department suggests that files be "backed up" to a network drive or external storage (e.g., CD, DVD, flash drive, Office 365 or external hard drive) to protect the data, and in the cases where a machine needs to be re-imaged, all the documents will be available to the user. Once the user logs into the district network there are several options of network drives available to store information. The most typical is the H:\ drive. This is the users' home drive and where IT suggests storing most information. This drive, like all network drives, is backed up centrally every night. The T:\ drive is the "global share" drive that is available for software installs and other needs for the entire district. Other drives may be available depending on your position and assignment.

How do I connect to Office 365?
1) Go to https://products.office.com/en-US/
2) Click Sign In (top right corner)
3) Put in your work e-mail address
4) Click Work or School Account
5) Put in your district password (same as logging into your computer)
6) Installation for Office 2016 is in the top right corner (not necessary for district PCs)

What software is currently installed on all computers?
-This is a list of the basic software currently installed on all district computers:

Windows 7 or 10 as an operating system
Office 2016
Adobe Reader
Flash Player
Internet Explorer (I.E.)
Firefox
Kaspersky – anti-virus program
Outlook - for teachers
Java
Infinite Campus shortcut
Real Player
QuickTime

HelpDesk icon
Shockwave

Some systems may have other software depending on the needs of the person in that position. If you are interested in evaluating or purchasing software for your district computer please follow the policy that is outlined in IIBG (see below – under Copyright).

What are the policies regarding computers in the district?
-The district policy that addresses most computer related issues is IIBG. Here is a copy of that policy:

IIBG ***Computer Use*** *(See GAA and JCDA)* ***IIBG***

Use of District Computers/Privacy Rights

District issued computer systems and electronic devices (including, but not limited to, Smartboards, iPads, iTouches, iPhones, eReaders, and eBooks) are for educational and professional use only. All information created by staff shall be considered district property and shall be subject to unannounced monitoring by district administrators. The district retains the right to discipline any student, up to and including expulsion and any employee, up to and including termination, for violations of this policy.

Copyright (See ECH)

Any request for new software shall be submitted on the district's Software Approval form and signed as approved by the Director of Technology (or designee). Software acquired by staff, using either district or personal funds installed on district computers or electronic devices must comply with copyright laws. Proof of purchase (copy or original) must be filed in the district office.

Hardware/Software

The Director of Technology (or designee) will approve the purchase of hardware or software. Staff shall not install unapproved hardware on district computers or make changes to software settings that support district hardware.

Installation

No software, including freeware and shareware, or other applications may be installed on any district computers or electronic device until cleared by the Director of Technology (or designee). The Director of Technology (or designee) will verify the compatibility of the software or application with existing software and hardware, and prescribe installation and de-installation procedures. Students shall not install software on district computers or computer systems. Program files must have the Director of Technology's (or designee) approval to be installed on any district server or computer.

IIBG Computer Use (See GAA and JCDA)IIBG-2

Equipment Connected to the Network

Non-approved district equipment (e.g., laptop, e-reader or other wireless device) will not be connected to the network or computing system without the signed Technology Code of Conduct by parent/guardian or responsible adult. This Code of Conduct will outline the responsibilities of the user and the district with respect to these devices. Any network device (e.g., printer, server, access point, hub/switch) is not to be installed without the prior approval of the Director of Technology (or designee).

Audits

The Director of Technology (or designee) may conduct periodic audits of hardware or software installed within the district to verify legitimate licensing and use.

Privacy Rights

Employees and/or students shall have no expectation of privacy when using district e-mail systems or any other official district communication systems. Any district e-mail, computer application, information in district computers, or computer systems is subject to monitoring by the administration. Only district business shall be conducted on district e-mail systems.

The district Information Technology department may remove faculty/staff information from district systems without notice (e.g., computers, laptops or servers) to allow for proper functioning of these systems. It is the responsibility of the faculty/staff member to maintain a backup of their information.

IIBG Computer Use (See GAA and JCDA)IIBG-3

Ownership of Employee Computer Materials

Computer materials, devices, software, or applications created as part of any assigned district responsibility or classroom activity undertaken on school time shall be the property of the board. Employees covered by the negotiated agreement shall follow procedures outlined in that document.

Lost, Stolen, or Damaged Computers and/or Equipment

Students and staff members may be responsible for reimbursing the district for replacement of or repair to district issued computers or electronic devices which are lost, stolen, or damaged while in the students' or staff members' possession.

Approved: 2/13

IIBGA Children's Internet Protection Act IIBGA

The district shall implement the Children's Internet Protection Act (CIPA). The superintendent shall develop a plan to implement the Children's Internet Protection Act. Such plan shall include measures to address the following issues:

(1) Access by minors to inappropriate matter on the Internet and World Wide Web,

(2) The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications,

(3) Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;

(4) Unauthorized disclosure, use, and dissemination of personal information regarding minors; and

(5) Measures designed to restrict minors' access to materials that may be harmful to them.

For the purposes of this policy, "minor" shall be defined to mean any student who is 18 years of age or under. The board charges the superintendent to develop the CIPA implementing plan so that all of the protections provided by this policy and the corresponding plan may be afforded to all district students.

This plan shall be on file with the board clerk and in each school office with Internet access, and copies shall be available. The superintendent shall ensure compliance with CIPA by completing Federal Communication Commission forms as required.

Approved: 2/13

PLEASE COMPLETE A HELPDESK TICKET (See Above) BEFORE MAKING CONTACT WITH IT STAFF ON DEVICE OR CONNECTIVITY ISSUES

Director of Information Technology

Dr. Mike Ribble	miker@usd383.org	Ex. 1004

Networking Department

Russ Dockins	russd@usd383.org	Ex. 1003
David Apgar	davida@usd383.org	Ex. 1001
Kevin Hollingshead	kevinh@usd383.org	Ex. 1002

PC Department

Thomas Brown	thomasb@usd383.org	Ex. 1006
Ben Kuehne	benk@usd383.org	Ex. 1007
Joshua Ransom	joshuahr@usd383.org	Ex. 1008
Eric Tallant	erict@usd383.org	Ex. 1009
Jose Triana	joset@usd383.org	Ex. 1005
Laura Hannan	lauraha@usd383.org	Ex. 1000

Infinite Campus/Database Support

Todd Bryant	toddb@usd383.org	Ex. 1860
Sandy Steck	sandys@usd383.org	Ex. 1861