Educational Technology
& Digital Learning

Martin County School District
2016-2017

Employee Handbook

Who We Are **3**
What We Support **3**
Security Awareness **3**
Data Protection and Physical Storage Guidelines **4**
Overview **5**
Email 5
Internet and WiFi 5
Logins and Passwords 5
Network Drives 6
Bandwidth 6
FOCUS 6
Curriculum Software 7
Computer Hardware 7
Support Services **7**
District-Purchased Online Resources **8**
Copyright Law-Teacher Guidelines **8**
Martin County Bring Your Own Device (BYOD) Responsible Use Guidelines **9**
Website Etiquette and Content Guidelines **10**
Email Guidelines **11**

Educational Technology (ET) is a support department. We are here to make your job easier. We are located at 500 East Ocean Boulevard in building 24 and can be reached at the extensions below.

Who We Are

Director of Educational Technology
Katie Preston x 30404

Coordinator of Computer Operations and Technical Support
Chris Hall x30379

Coordinator of Administrative Technology
Paul McGuinness x30361

Coordinator of Digital Learning
Douglas Konopelko x48141

Digital Learning Specialist
Jessica Falco x48142

Help Desk x30359

What We Support

- Desktop PCs
- Laptops
- Printers/scanners
- Telephone systems
- *MS Office* software
- Spam blocking
- Virus protection
- Data Security
- Enterprise applications
- Site 2-way radios
- Administrative software
- Instructional software
- Classroom technology
- Email
- Internet access
- Content filtering
- Remote access
- WiFi solutions
- Network Security
- Public safety radios

Security Awareness

- Never leave your computer unattended unless it is locked or logged off.
  A shortcut for quickly locking your computer is to hold down the Windows icon key (located next to the Alt key on your keyboard) and then press the letter L. To unlock your computer, press Ctrl+Alt+Delete and then enter your password.
- Protect your passwords and never share them. If asked for your password, say "No".
- Guard electronic data as you would hardcopy. For more information about what data should be protected, read the Family Rights and Privacy Act (FERPA) http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html and the Health Insurance Portability and Accountability Act (HIPAA) http://www.hhs.gov/ocr/privacy/index.html.

- Monitor the electronic activity of students in your care. No web filter is perfect as hundreds of new websites are created every day.
- Educational Technology monitors Internet and email use and conducts random audits throughout the year for appropriate use.
- Report security violations and concerns to your supervisor.
- Become familiar with School Board Rules including the 7540 series:
  - 7540 Computer Technology and Networks
  - 7540.01 Technology Privacy
  - 7540.02 District Web Page
  - 7540.03 Student Network and Internet Acceptable Use and Safety
  - 7540.04 Staff Network and Internet Acceptable Use and Safety
  - 7540.05 Electronic Mail
  - 7542 Access to Technology Resources from Personal Communication Devices
  - 7543 Utilization of the District's Website and Remote Access to the District's Network

Data Protection and Physical Storage Guidelines

1. Student data should be secured, no matter the location or device, in compliance with FERPA regulations and/or any other applicable State and Federal guidelines.

2. Health information of employees or students should be secured, no matter the location or device, in compliance with HIPAA regulations and or any other applicable State and Federal guidelines.

3. Documents can be emailed safely if no one on the distribution list is outside our domain (@martin.k12.fl.us). However, documents to any address outside of our domain (@gmail.com, @FLDOE.edu, etc.) must be encrypted and password protected if they contain sensitive or protected information. Encryption requires a product plus knowledge & communication between the sender and the receiver.

4. Any protected data that needs to be stored outside where it normally resides and accessed via a workstation should only be stored on a user's personal F drive or in a protected folder located on a network server. Never store protected data directly on a workstation (this includes the PC's desktop and the C Drive), or in an unprotected or commonly used folder that is accessible to others.

5. Protected data should never be stored on a laptop.

6. Portable media (e.g. USB thumb drives, flash memory cards, CD or DVD, etc) should not be used for storing protected data. If it becomes necessary to use portable media to transport protected data, make sure to delete the protected data from the media as soon as transport is complete. If the protected data was placed on a CD or DVD, destroy the CD or DVD. Most paper shredders are capable of shredding a CD or DVD.

7. When equipment is transferred or disposed, all hard drives are formatted and wiped. The Purchasing/Warehouse department complies with all USDOD standards when disposing of computer equipment.

8. All hard copies of protected data should be stored in a secure location.

9. Any hard copy of protected data that has become obsolete must be shredded and disposed of in compliance with State and Federal regulations.

Overview

Email

Most employees are given an email account and access to the Internet. Please refer to School Board Rules above and the Acceptable Use Policy below. Do not email private information about students (see FERPA and HIPAA) unless you are able to encrypt it. Most usernames are the first six letters of the last name, followed by the first initial. For new employees upon first log-in, see your media specialist or call the Help Desk (30359) for the default password. You will then be prompted to change your password. Follow the on-screen directions.

Internet

The District uses a role-based Internet filter to block inappropriate material; however, if you are a teacher, it is your responsibility to constantly monitor what students are doing online.

WiFi

WiFi connectivity is available in all classrooms, the media center, administration areas, gyms, auditoriums and cafés. Corridors and outdoor areas are not covered. You may be able to connect in these non-covered areas however, reliable coverage is not assured.

Students and staff may connect wireless devices to the **MartinSchools** Wi-Fi network. All employees will use their network user id and password to access the MartinSchools Wi-Fi network. Students will use their student id and password to access the MartinSchools Wi-Fi network.

On a yearly basis, every student must return a completed signed parent and student acknowledgement form #356. Once FOCUS is updated indicating the form was received, network access is typically enabled within one business day.

Guest WiFi is available for non-district persons and must be arranged by submitting an iSupport ticket 48 hours in advance.

Logins and Passwords

Passwords should be complex and have a minimum of 8 characters. For a password to be complex, three of the four following characteristics must apply:

1) At least one character is an uppercase letter
2) At least one character is a lowercase letter

3) At least one character is a number (0-9)
4) At least one character is a symbol (for example, !, #, }, $, %, or other non-alphanumeric characters)

Some examples of passwords that would comply with the new policy (at least 8 characters and complex) are: Jibber923, Jabber4%4, piperF0v or ApplePie#.

Some users like to use phrases, nursery rhymes or song lyrics, substituting numbers or symbols for letters. For example, Pop!Goes (Pop goes the weasel), Blackb1rd or S1ng1ng (Blackbird singing in the dead of night) or EveryR0se (Every rose has its thorn).

Some password examples:

Bad	Good	Better
Fido44 (too short)	Fido4u4u	Fido4F0UR
PopGoes (too short, no symbol or number)	Pop!Goes	Pop!GoestheWeasel!
cassidy7 (no uppercase or symbol)	Cassidy7	C4ss1dy7

It is important to protect your password:

- Keep your password in a safe place.
- Do not share your password.

You will be prompted to change your password every 60 days. Remember, you are accountable for your password and all activity associated with it. Never share your username and password with anyone.

Network Drives

- Use your F drive for storing documents and data that you wish to keep.
- The F drive is your personal drive (for business use only) and it is backed up nightly.
- Common drives at each school site are G for shared documents and S for student work. There is also a W drive that is for ET's use only.
- Do not store sensitive student data on any shared drives (G, S, etc.).

The C drive (local hard drive) is NOT backed up. Anything stored on your C drive (this includes anything placed on your Desktop screen) may be erased without notice.

Bandwidth

All school sites are connected to the Internet via fiber or Metro-E connection; however, bandwidth is limited and should be used for business purposes only. Please do not stream music (such as Pandora, I(heart)Radio, or Sirius) over the Internet.

FOCUS

FOCUS is the student information system, electronic gradebook, and parent portal used by everyone in our District. NEVER LEAVE YOUR FOCUS DESKTOP UNATTENDED! For help:

- For **School Based Support**, contact your Attendance Manager or Gradebook Manager
- For **System Support**, email Focus_Help (email through Outlook)

Curriculum Software

All curriculum software must be approved by Instructional Services (IS) and Educational Technology (ET) departments *before* purchase and/or installation. See Form #1082. No outside or donated disks or CDs are to be used on District computers.

Computer Hardware

All computer hardware must be approved by Instructional Services (IS) and Educational Technology (ET) departments *before* purchase. See Form #1178. This includes donated hardware.

Support Services

iSupport is the fastest, most efficient way to receive technical support. Enter your own ticket using the iSupport icon on your desktop. If you require emergency support, please enter a ticket and call the ET Help Desk (Ext 30359) referencing the ticket number just created.

The **Digital Learning Community (DLC)** is our professional learning network. User groups meet monthly during the school year. CampTEACH (Technology Empowering Academic CHange) sessions are held during the year and each summer for supplemental technology training and are available for all teachers. See your DLC leader for information on this District program.

Supplies: MCSD negotiates prices from vendors to give our schools buying power. These items are stored in the warehouse at the Service Center and are available for you to purchase through your school monies (Adopt-a-Classroom, EES, PTA, etc.) The warehouse catalogue is available on Outlook. To access this folder, navigate to *Public Folders→All Public Folders→District Internal Documents→Warehouse*. Instructions and catalogue are included.

Printing: Use classroom printer when printing fewer than 5 pages or for emergency class sets when you can't leave the classroom. Use shared printer for color jobs of less than 5 pages and monochrome jobs of less than 15 pages. The most cost-effective solution for jobs of 15 pages or greater is utilizing the Reprographics service. See your media specialist for the latest form and procedure for submitting a job to Reprographics.

A Teacher Website is generated for all educators in FOCUS. You can utilize FOCUS, EdLine, or Google Sites to create your teacher website. If you wish to create a classroom website, please read School Board Rule 7540 and contact the Coordinator of Digital Learning or your school webmaster.

Grants: All teachers are encouraged to seek out grant opportunities. Contact the Education Foundation (219-1200 x 30417) for information on teacher grants.

Use of Movies and Videos: See School Board Rule 2540 and below for specific details on licensing.

District-Purchased Online Resources

Resource	School Access	Home Access
ClassLink	ClassLink can be used to access most other district materials and can be found at: http://launchpad.classlink.com/martinschools Use your network credentials to access	Same as school
Google Apps for Education	www.google.com drive.google.com classroom.google.com networkcredential**@sbmc.org** Initial password is 8 digit employee ID	Same as school
Britannica Online Encyclopedia	http://school.eb.com no username or password required	http://school.eb.com Username: martincounty Password: learn
Safari Montage	http://safari Use your network credentials to access	http://safari.martinschools.org
Professional eLibrary	http://galesites.com/ascd/martin/# No username or password required There is a direct link off our webpage under Employee Tab	http://galesites.com/ascd/martin/# Password: Professional
Florida Electronic Library	http://galesites.com/menu/index.php?loc=fl_martincntysd No username or password required There is a direct link off our webpage under Parents & Students Tab	http://galesites.com/menu/index.php?loc=fl_martincntysd Password: student

Copyright Law-Teacher Guidelines

For more information about copyright, please visit : http://bit.ly/digitallearningmcsd

Martin County Bring Your Own Device (BYOD) Responsible Use Guidelines

Technology is one way of enhancing the District's mission of teaching students to be productive, college- and career-ready members of the 21st century. In order to increase the use of technology in the classroom, Martin County Schools are implementing a BYOD program. We want students to embrace appropriate use of technology so they may become responsible digital citizens.

Definition of BYOD
Bring Your Own Device allows students to bring and use their own personal technology device to connect to the District wireless network and Internet for use during classroom instructional activities directed by instructional personnel. For the purpose of this program, the word "device" will include: Wi-Fi enabled devices including but not limited to cell phones, iPads, iPod Touches, laptops, e-readers and Android tablets.

Internet Access and Use
The District will provide secure and filtered access to the internet through the District wireless network. Usage of the District wireless network account is encouraged. The District is not liable for content that is accessed or charges that may be incurred if a student chooses to use his/her personal data plan to access the internet.

Security and Damages
Each user is responsible for his/her device and is expected to use it appropriately. Responsibility to keep personal technology secure rests with the individual owner. Martin County School District is not liable for any device stolen or damaged on campus. Martin County School District will NOT replace or provide financial restitution for any stolen or damaged personal electronic device. If a technological device is stolen or damaged, the issue will be handled through the administrative office similar to other personal artifacts that are impacted in similar situations.

BYOD Student Agreement
The use of technology to access educational material is a privilege. When abused, privileges will be revoked and disciplinary consequences will be issued. When respected, these privileges benefit the learning environment as a whole. Students and parents/guardians participating in the BYOD program must adhere to the Student Code of Conduct, as well as all Board policies, particularly the Student Responsible Use agreement. Additionally, all mobile devices:

- Must be in silent mode while on school campuses and while riding school buses.
- Students are not allowed to use any device to photograph or record (either in audio or video format) another person on school property at any time without that person's permission.
- Devices may not be used for any purpose that promotes academic dishonesty.
- Students will not participate in behavior utilizing their personal device on or off campus that "materially or substantially interferes with school operations" and/or creates a "substantial disruption to the educational process". If such behavior occurs, disciplinary action will be issued as deemed appropriate by the MCSD Code of Conduct and School Student Handbook.

Students and Parents/Guardians acknowledge that:

- The school's network web filter will be applied to a device's connection to the internet and any attempt to bypass the network filters is prohibited.
- Students are prohibited from processing or accessing information by "hacking", altering, or bypassing Martin County School District network security policies.
- The District has the right to collect and examine any device if a student is suspected of violating the BYOD guidelines.
- The charging of devices is the responsibility of the student and teachers may allow or disallow that privilege at their own discretion.
- The District is not responsible for lost, stolen or damaged personal technological devices.
- The District is not responsible for maintenance or repair of any personal technology.
- The District is not responsible for any costs incurred due to use of personal technology.
- Printing from personal devices will not be supported at school.
- Each teacher has the discretion to allow and regulate the use of personal devices in the classroom and on specific projects.

Website Etiquette and Content Guidelines

Etiquette

The purpose of having a website is to inform, communicate, and build relationships with our students, parents, and community. Websites make an impression and you will be judged on the quality of your writing as well as the overall look, feel, and function of your site. Some guidelines to follow include:

- Refrain from using backgrounds, animated gifs, and sounds (including music).
- Always have a colleague proofread your content before publishing it.
- Keep the content fresh.

Content

If someone other than a District employee maintains a web site about the District, school, or students, the content of all pages must be approved by the school's principal or his/her designee.

Links

In order to provide the community with a clear understanding of what is or is not District-sanctioned or District-affiliated, all links that direct users to outside of the District (external links) should go through the District's disclaimer. It is the responsibility of each site's administrator (Principal) to make sure links are provided only to appropriate external websites. See the *Policy and Procedure for Link Monitoring* for more detailed information.

Absolutely No:

- student photographs on teacher websites (school home page or link to a newsletter is permissible with proper parent release)
- identifiable student work displayed (e.g. pictures of artwork are acceptable)

- use of copyrighted materials (text, sounds, or graphics)
- commercial advertising
- political lobbying

Email Guidelines

Most employees are provided with District e-mail accounts to improve the efficiency and effectiveness of communication both in and outside the organization. Although e-mail has become a valuable communication instrument, it is important to remember that it is not a secure and confidential method of communication.

Guidelines to Using E-mail:

- Never discuss, inquire about, or inform others through e-mail any sensitive student or employee information, including anything related to grades, discipline, medical or health issues.
- E-mail must never be used to discuss contentious, sensitive or confidential issues. These issues should be dealt with face-to-face or by phone.
- Consider your audience before forwarding emails. For example, it is usually NOT appropriate to forward an email conversation string involving one group of employees to another. Principal conversations should not be forwarded to teachers.
- E-mails that reside on the District servers are not confidential. E-mail messages may be requested by the public and may, unless they are exempt under the law, be open to public inspection.
- E-mails should be brief and to the point and sent to accomplish a specific task.
- Use "Reply All" only when you are compiling results or need collective input.
- Avoid sending "thank you" e-mails to acknowledge receipt of an e-mail.
- Do not e-mail large files such as pictures.
- DO NOT USE backgrounds, animated gifts, quotes in the address line or nonstandard fonts.
- E-mail is for business use only.
- Your e-mail is a reflection of you and the District.

Resources

School Board Rules http://www.neola.com/martin-FL/
Family Rights and Privacy Act (FERPA)
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Health Insurance Portability and Accountability Act (HIPAA)
http://www.hhs.gov/ocr/privacy/index.html