A Guide to safe, secure, and acceptable use of computers and related technology for staff of the School District of Osceola County, Florida

EMPLOYEE TECHNOLOGY AWARENESS AND SECURITY HANDBOOK 2024-2025

SDOC Leadership Approved

TABLE OF CONTENTS

TABLE OF CONTENTS 2

PURPOSE 3

INTRODUCTION 4

COMPUTER USER RESPONSIBILITIES 5

ELECTRONIC SECURITY 6

PHYSICAL SECURITY FOR DISTRICT COMPUTERS 9

DATA STORAGE 10

DATA PROTECTION AND SECURITY 11

SOCIAL NETWORKING 20

DISTRICT SCHOOL/DEPARTMENT WEBSITES 21

U. S. COPYRIGHT LAWS 21

USING TECHNOLOGY WITH STUDENTS 22

ELECTRONIC COMMUNICATIONS 24

PERSONAL DEVICES 28

PURCHASING GUIDELINES 30

LEGAL INFORMATION 30

PURPOSE

The purposes of the Employee Technology Awareness and Security Handbook:

1) Define guidelines for employees in the proper use of technology resources (hardware, software, and network) in the District in order to minimize the risk of harm or damage to these systems and essential data due to inappropriate use or breaches of computer security.

2) Document the security policies that have been implemented to protect and secure the technology resources of the District

This handbook is subordinate to any collective bargaining agreement, employment contract, or other employment agreements. It is expected that all users, especially administrators and those responsible for computer installations, software implementations or support (e.g. Technology Contacts, Technology Specialists, or Media Specialists), be familiar with this handbook.

Any questions or suggestions for further improvements to this handbook may be forwarded to the District's Chief Information and Technology Officer.

INTRODUCTION

Maintaining current technology is vital to the effectiveness and efficiency of District operations. Enhancements to technology resources are expensive and time consuming, but these tools provide unprecedented opportunity for both students and employees to succeed. However, it puts the District at considerable risk to implement new technologies without established policies and practices in place.

- Employee Technology Awareness and Security Handbook
- Employee Technology Awareness & Security training
- Network Acceptable Use Policy, School Board Rules, 8.60+
- Social Media, School Board Rules, 8.601+
- Employee Use of Cellular Telephones, School Board Rules, 6.321+
- Copyrighted Materials, School Board Rules, 3.52
- Prohibited Interaction with Students, School Board Rules, 6.84
- Gifts of Computers and Technical Equipment, School Board Rules, 7.79
- Student Use of Personal Technology, School Board Rules, 8.63+
- Student Internet and Network Use Procedures, FC-820-2259
- Employee Relations – Civility, School Board Rules, 6.392*
- Gifts to Employees, School Board Rules, 6.96
- Internet Safety, School Board Rules 8.602*+
- Artificial Intelligence Acceptable Use, School Board Rules 8.603+
- Operation of Unmanned Aerial Vehicles (Drones), School Board Rules 8.64

COMPUTER USER RESPONSIBILITIES

Employees are responsible for the appropriate use of District computers and communications resources and for taking reasonable precautions to secure the information and equipment entrusted to them. Employees are responsible for reporting inappropriate use of District computers and breaches of computer security. Employees are responsible for adhering to policies and practices as described herein, and in other policies and procedures to ensure that computer and communication resources are used acceptably and that practical measures are taken to prevent loss or damage of computer information and equipment.

Changes in Employment Status
All programs and data on employee computers are considered District property. Deleting, altering, or sharing confidential, proprietary, or any other information upon termination is prohibited.

The following activities are prohibited upon terminating employment, and will be prosecuted to the full extent of the law:

- Accessing District computers, network resources, or web-based applications/programs
- Providing third parties, or anyone else, access to District computers
- Copying, removing or destroying computer files, data, programs, or computer equipment

Unauthorized Changes to District Computers
Installing software and making changes to computer hardware, software, and system configurations could disrupt or replace essential applications.

Do not install software or programs on any District computer without authorization. Apps in the company portal are approved and users can install the apps from the company portal. If there are apps on the approved list of software and web tools available through Microsoft, an employee can submit a ticket in Incident IQ to add the app to the company portal. Employees are permitted to install printer software if the laptop is used at home. Software or programs loaded on District computers must be licensed to the school and/or department of the District. Failure to comply with any software licensing requirements is a serious violation of the law, and could result in discipline up to, and including, termination and criminal charges.

ELECTRONIC SECURITY

Unauthorized Access

Unauthorized access of computers (hardware and software) and communication resources (e.g. Internet access, web servers, e-mail) is prohibited. Unauthorized access to data files and automated systems is prohibited. Accessibility is not to be confused with authorization. Employees may have access to data files and automated systems but this is not the same as having authorization to access the data files or automated systems.

Any form of tampering, snooping, or hacking to gain access to computers is a violation of District policy and carries serious consequences, up to and including termination and criminal charges. Employees are required to secure their computer when not attended and turn it off at the end of each day.

During work hours, if an employee walks away from his/her desk, he/she is required to "lock" his/her computer to secure it from unauthorized use. With a Windows operating system, this is done by simultaneously pressing the Ctrl+Alt+Delete keys and selecting the "Lock computer" option on the screen. Computers may also be locked by simultaneously pressing the Windows key (next to the Alt key) and the letter "L".

Passwords

A user ID and password combination securely identifies and authenticates an employee for system and data access. Without the use of complex passwords, constructed according to a proper protocol, the security that a password provides quickly fails.

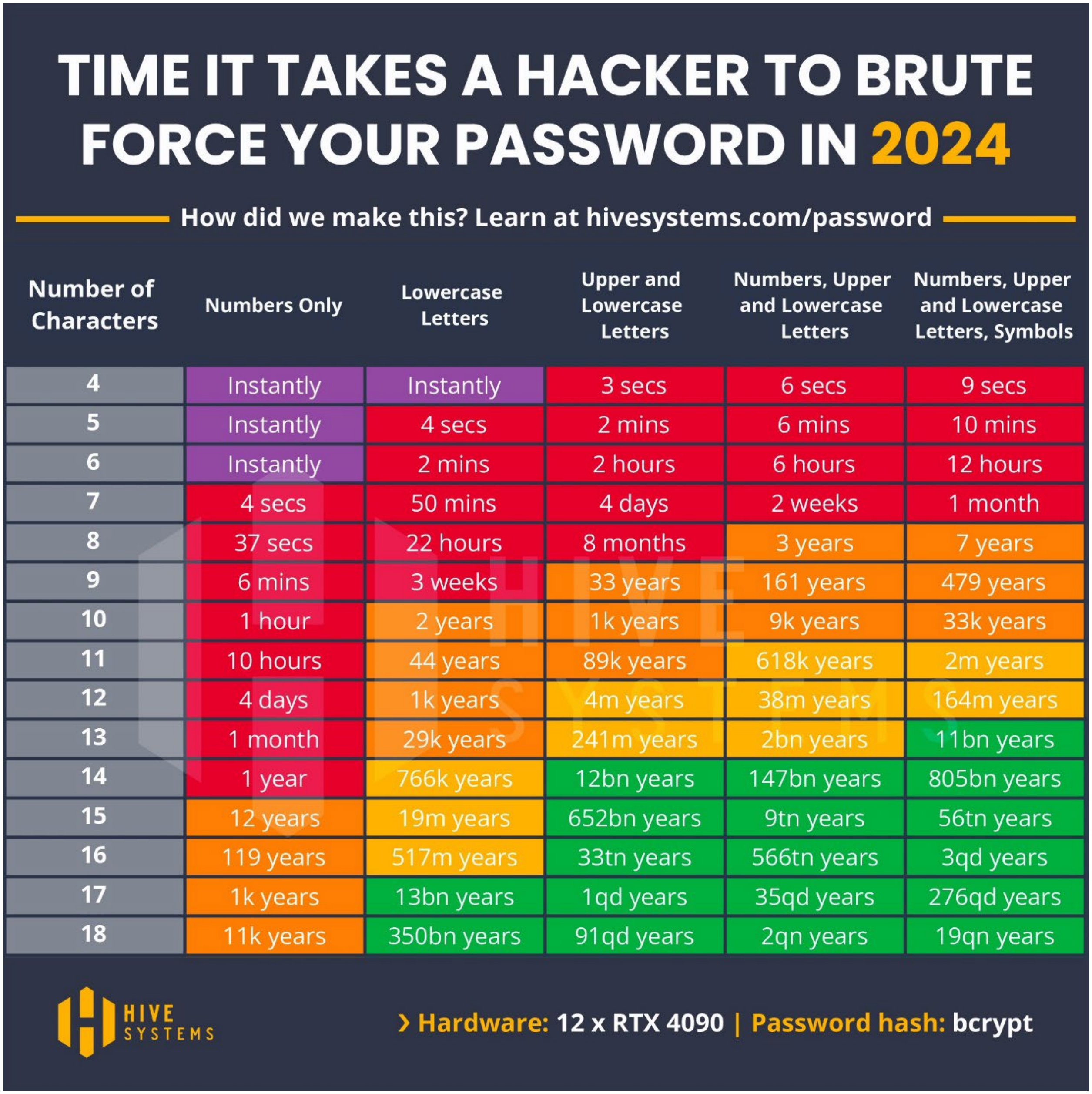
Password Selection

Effective July 10, 2024, the minimum character requirement for all employee passwords has been increased from 8 characters to 14 characters. The next time your password expires following this date, the new password must meet the new 14 character minimum requirement.

The rest of the password policy remains the same:

- Passwords are composed of at least fourteen (14) characters.
- Passwords should contain a mix of uppercase letters, lowercase letters, and numbers or special characters.
- Passwords cannot contain common words, phrases or personal information.
- Passwords must be changed every 90 days.

Look at the chart below and check the strength of your password. The goal is to have your password in the green area! www.hivesystems.com/password



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

> Hardware: 12 x RTX 4090 | Password hash: bcrypt

Protecting Passwords

User IDs and passwords are not to be shared with anyone. Do not write them down where someone can find them. Do not send them over the Internet, Intranet, e-mail, or any other communication line. Do not use any automatic log in features to save password information for accessing any District system.

Do not log in using a District user ID and password in order to allow another person access to any computer, network, software, or data. If another person needs access, he/she must obtain his/her own user ID and password.

For example, teachers are not to log in to any classroom student computer using the teacher's District user ID and password. Using a teacher log in on a student computer gives any student using that computer full access to all of the teacher's files and records.

Do not ask someone for his/her user ID or password. Do not attempt to ascertain another employee's user ID and password under any circumstances. This is a violation of District policy and carries serious consequences, resulting in discipline up to, and including, termination and criminal charges.

Classlink, a single sign-on solution, is provided by the District to provide secure access to applications using only your active directory username and password. By using Classlink, users only need to remember their active directory credentials.

Password Resets

Your password can be reset for the Finance and Payroll Systems through the District's secure Employee Portal. You can access the Employee Portal through Classlink or use the link below:
https://employees.osceola.k12.fl.us

Contact the Help Desk at 407-870-4000 or extension 67000 with other password reset requests.

Harassment, Threats, and Discrimination

Refer to School Board Rule, Employee Relations – Civility, 6.392 . There is no expectation of privacy with any SDOC communication with the exception of student data.

External Access

Important, confidential, and proprietary information is stored on District computer systems, so only District personnel are allowed access to these computer systems. The Chief Information Officer, or his/her designee, is authorized to determine vendor access privileges for vendors under contract with the District.

PHYSICAL SECURITY FOR DISTRICT COMPUTERS

Locks

Computers are to be locked or turned off when not attended. Locking the door to the employee's office or classroom is a good practice of physical security. It is recommended that laptop computers and devices be secured in a locked file cabinet or locked closet.

During work hours, if an employee walks away from his/her desk, he/she is required to "lock" his/her computer to secure it from unauthorized use. With a Windows operating system, this is done by simultaneously pressing the Ctrl+Alt+Delete keys and selecting the "Lock computer" option on the screen. Also, computers may be locked by simultaneously pressing the Windows key (next to the Alt key) and the letter "L".

Computers and Electronic Devices

There are many sensible measures that can help reduce the risk of loss and/or damage. The following procedures are to be followed when a District device is used off-site:

- Current District borrower's form must be on file with school or department (FC-220-0894)
- Back up all important District files on the departmental "Q" drive or staff resource shared drive (see Data Storage section for more information)
- Use equipment only for work-related, educational activities
- Safeguard devices against accidental damage and theft
    - Always transport and store devices in a concealing, padded computer carrying case
    - Do not leave devices in plain sight in a vehicle
    - Do not leave devices in any vehicle exposed to extreme temperatures
- Report lost or stolen devices immediately to law enforcement, obtain a police report, and notify the site or department administrator/supervisor
- Do not allow family, friends, associates, and others access to District devices for any purpose
- Return device(s) to work location on a daily basis, with exception of travel for work related purposes
- Adhere to the same policies and practices of the District for on-site use

DATA STORAGE

Network Storage

There are network storage drives available to all District employees for the purpose of saving important documents and data. These drives are secure, available only within the District's local network, and are regularly backed up. This available storage is not to be used for archiving large amounts of non-critical or personal files.

Individuals and departments with access to shared drives should employ the following management practices:

- No storage of personal files (non-District related) on the staff resource shared drive
- Do not save executable (.exe) files on the staff resource shared drive
- Do not store movies, music or images on the staff resource shared drive

Folders were created in the "Q" drive with a retention time for items that were previously boxes for storage. A "Daily Files" folder was created for any other items that do not have a retention time. All folders that contain documents that do not have a retention time should be placed under the "Daily Files" folder.

Please contact Records Management when setting up folders with a retention time.

The District provides alternative storage for sizeable projects or files suitable for educational purposes. To request additional storage, please create a ticket inIncident IQ.

Data Storage-Outside of the District Network (the Cloud)

The "public cloud" is a remote computer to which files and/or data are uploaded. This type of storage device is owned by a third party, and not sanctioned by the District for employees to use for District business. The most common "public clouds" include, but are not limited to, iCloud, Evernote, Dropbox, or GoogleDrive.

All employees have been provided with a District Microsoft Office365 OneDrive account for District business. District provided Office365 accounts may use OneDrive to temporarily store files containing student-identifiable or employee-identifiable information as Microsoft provides a highly secure service and is FERPA compliant. Long-term storage of files containing student data or other confidential information should be stored on the departmental "Q" drive or staff resource shared drive.

Use of GoogleDrive and Dropbox

With approval of the Chief Information and Technology Officer, other cloud storage services including but not limited to GoogleDrive and Dropbox may be used with outside governmental agencies for special projects. For example, sometimes the Florida Department of Education places documents in Dropbox for distribution to Districts throughout the state. Once approval has been granted, the Chief Information and Technology Officer or his/her designee will provide requirements and procedures to use these public cloud services.

Removable Storage

OneDrive is a resource the District has approved to eliminate the need for thumb/flash drives.

If thumb drives or portable storage devices are received from a local, state, or federal government agency, the information on these devices may be transferred to District equipment. However, if thumb drives or portable storage devices are received from any other third party, including but not limited to non-profit organizations or business vendors, these devices shall be scanned for viruses with the District's currently updated virus scan software prior to employee use.

For assistance in scanning portable storage devices, contact your school's computer technician. District employees should contact the Help Desk at 407-870-4000 or extension 67000.

- *The only current exception to this policy for students shall be Exceptional Student Education or Section 504 students whose Individual Education Plans or Section 504 Plans specifically state that the use of a thumb drive or portable media storage device is an allowable accommodation for classroom instruction.*

DATA PROTECTION AND SECURITY

Deletion of Electronic Files

Electronic versions of records fall under the same records retention and destruction guidelines and rules as "hardcopy" records. Permanently deleting District records may be a violation of state or federal statutes. Please consult the District's Records & Forms Management Manual for answers to questions regarding records destruction.

Retention of Electronic Files

Employees shall adopt an electronic file structure to store electronic records and information for easy access and preservation. Records that have a retention time should be stored in the Records Management folder which can be located in your shared drive. Each folder should contain records that have the same retention requirements and labeled with the General Records Schedule title. When annual destruction is conducted, the yearly folder will be deleted by the Records Department. It is the responsibility of the Department or School to ensure that documents in these folders do not need to be kept beyond their retention time due to pending litigation or other reasons. Full instructions can be found in the Records and Forms Management Manual located in SDOC Resources under Records Management.

The following are practical guidelines for organizing electronic files:

- Create a folder with the General Schedule title of the record
- Create a sub folder for each school year
- Create separate sub folders for organizing the documents under the GS category and school year

Accidents, Mistakes and Spills

According to current research, most data loss and damage to computers is done by authorized users. Mistakes and accidents represent the biggest cost when it comes to computer information loss.

Give careful attention before deleting, saving, or transmitting files. Employees need to take reasonable precautions with respect to computer operations, maintenance, handling, and transportation. Avoid placing liquids and other food items near computers.

Personal Use of Computers

Incidental and occasional personal use of District computers during breaks and lunch time is permitted, with the exception of the prohibited activities below. If an employee considers it awkward to ask permission about a specific activity, it is probably not an appropriate use of District computers. If uncertain, contact an administrator/supervisor.

Prohibited activities include, but are not limited to:

- Using large amounts of bandwidth such as in streaming audio or video
- Computer games
- Personal software and hardware
- Storing personal photos, music, or videos
- Storing executable files
- Gambling or any other activity that is illegal
- Operating a personal business

- Storing or transmitting inappropriate or sexually explicit images, videos, jokes, junk mail, chain letters, etc.
- Soliciting for commercial, religious, charitable, or political causes

Proprietary Information

District data, databases, programs, and other proprietary information represent District assets and are strictly to be used for authorized District business. Use of District assets for personal gain or benefit is prohibited. Sharing District proprietary information with District personnel, or third parties, is prohibited.

Confidentiality

Student data, information, and records are confidential. Unauthorized employee access to these records is strictly prohibited. Confidential information should only be used for its intended purpose. Accessibility is not to be confused with authorization. Though an employee may be able to access, read, or print out student information on a District computer or on shared drives on the network, he/she is responsible for using student information in which he/she has a "legitimate educational interest." For more information related to confidentiality, refer to the Family Educational Rights and Privacy Act, (FERPA), the federal law that protects the privacy of student education records. Florida Statute 1002.22 states that education records shall be protected in accordance with FERPA.

Handling Confidential Information

Confidential information stored on computers is typically more difficult to manage than traditional paper documents that are sealed in an envelope and locked in a filing cabinet clearly labeled CONFIDENTIAL. As such, it is important that employees take extra care with confidential information stored on computers.

The following are ***inappropriate*** under normal circumstances when dealing with confidential information:

- Printing to a printer in an unsecured area where documents may be read by others
- Reading documents printed by others to a shared printer
- Leaving a computer, with confidential information visible, unlocked while unattended
- Leaving computer media (disks, CD's, USB drives, etc.) with confidential data unattended and easily accessible
- Sending confidential information over non-secured Internet or other network connections, including posting of grades for parental or student access

- Storing confidential student data files (including back-ups) in an unsecure location, available to unauthorized users

Appropriate security procedures are essential. These typically include user authentication and authorization, encryption or protection of the transmission packets, and access records with strict controls. Contact the Help Desk at 407-870-4000 or extension 67000.

Computer Sabotage

Destruction, theft, alteration, or any other form of sabotage of District computers, programs, files, or data is prohibited and will be investigated and prosecuted to the full extent of the law.

Viruses, Worms, and Trojan Horses

Virus protection is installed on all District computers and various safeguards are used for the District network. All incoming and outgoing e-mail is scanned for viruses and other malware. Tampering with or disabling the anti-virus program is prohibited.

It is critical that employees ascertain that data and software to be installed on District computers are from a trusted source and free of viruses. Viruses can result in significant damage to systems and lost productivity. If uncertain, contact the local school Technology Contact or the Help Desk at 407-870-4000 or extension 67000.

Use of known viruses, worms, or Trojan horse programs is prohibited. If a virus, worm, or Trojan horse, or what is suspected to be one, is identified, do not attempt to fix the problem. Immediately turn the computer off, make notes as to what was observed, and contact the Help Desk at 407-870-4000 or extension 67000. Do not open attachments or links from unknown or suspicious sources including anything suspicious from people known to you.

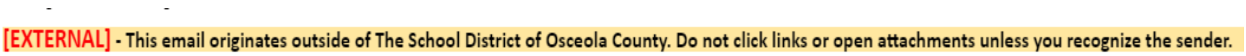
The principle objective is stopping the contamination before additional damage occurs. Viruses are designed to travel. The key to containment is limiting the reach of the contamination. If you suspect your device is contaminated, you need to unplug the network cable and/or remove the device from the wireless network. Then, contact your school tech or the Help Desk at 407-870-4000 or extension 67000.

Phishing Email

Phishing emails are one of the most common ways for malicious hackers to gain access to your online accounts, plant malware on your device, or even convince you to make unusual purchases. By posing as a legitimate or trusted sender, a threat actor tries to trick victims into clicking malicious links, downloading attachments, or replying to their emails.

If you receive a suspicious email or text message asking you to click on a link or open an attachment, the most important thing is to NEVER click these links or download attachments. Ask yourself this question: Do I have an account with the company or know the person that contacted me?

The School District of Osceola County has implemented means to help you identify emails that do not originate from within the district. Emails that originate from outside the district will have the distinctive external banner flag present at the top of the message. Below is an example of the external banner flag:



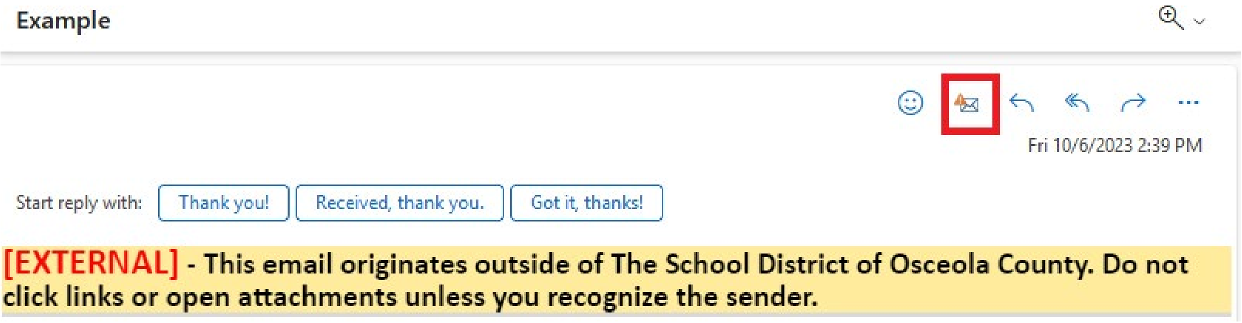
[EXTERNAL] - This email originates outside of The School District of Osceola County. Do not click links or open attachments unless you recognize the sender.

The School District of Osceola County also encourages users to send suspected phishing emails to the email security team. This allows our staff to analyze the email and improve our spam filters, thereby improving the safety of the school district's community. Please read below, follow the steps to report any suspicious emails, and help fight the scammers.

It is important that you report the ORIGINAL email you received. Please do not forward phishing emails to anyone within the School District.

To report phishing in the Microsoft Office 365 web browser:

1. Click on the Phish Alert – Report Phish app located at the top of the message.

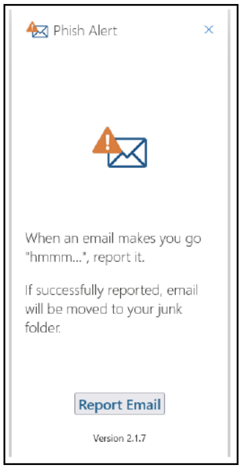


Example

Fri 10/6/2023 2:39 PM

[EXTERNAL] - This email originates outside of The School District of Osceola County. Do not click links or open attachments unless you recognize the sender.

2. A popup window will appear asking for your confirmation to report this email to our security team. Click on “Report Email” to send the message to our team.



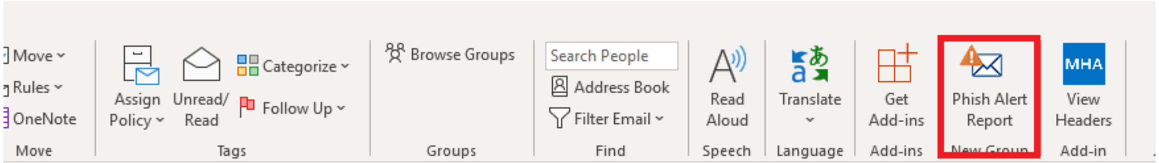
Phish Alert

When an email makes you go "hmmm...", report it.

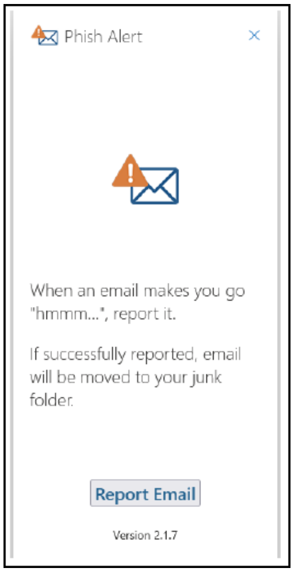
If successfully reported, email will be moved to your junk folder.

To report phishing in the Outlook client app:

1. Click on the “Phish Alert – Report Phish” button at the top right of the suspicious email.



2. A popup window will appear asking for your confirmation to report this email to our security team. Click on “Report Email” to send the message to our team.



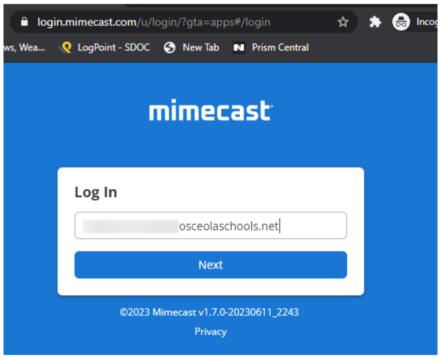
Phish Alert

When an email makes you go "hmmm...", report it.

If successfully reported, email will be moved to your junk folder.

Mimecast Email Security – Personal Portal

Working with Mimecast, our email security provider to protect our staff mailboxes, we might come across some emails that could potentially be placed ON HOLD as they could be categorized as spam mail, junk mail, or what may be considered as “grey mail.” These messages can now be reviewed, and staff will be able to determine if these messages being held should be blocked - meaning you won’t receive them anymore or you can release and permit the sender or domain. This will set up an allow for your mailbox (not everyone) for these emails to go to your inbox going forward. You will receive an email from Mimecast notifying you if you have messages on hold with a link to the login portal, or you may visit https://login.mimecast.com and sign-in with your @osceolaschools.net email address as shown below:



login.mimecast.com/u/login/?gta=apps#/login

mimecast

Log In

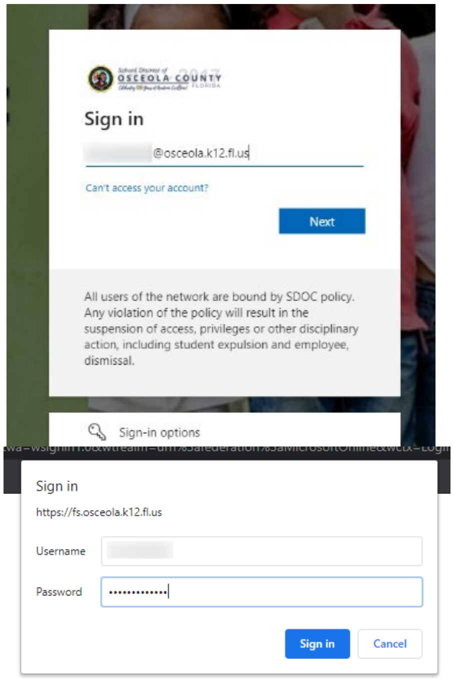
[redacted]osceolaschools.net

Next

©2023 Mimecast v1.7.0-20230611_2243

Privacy

If you are signed-in at a district computer as yourself, you will automatically be signed into Mimecast. If you are on a personal device, there are two additional steps. You will be directed to our Office 365 login page where you will use your @osceola.k12.fl.us address and then enter your username and password as shown below:



Sign in

[redacted]@osceola.k12.fl.us

Can't access your account?

Next

All users of the network are bound by SDOC policy. Any violation of the policy will result in the suspension of access, privileges or other disciplinary action, including student expulsion and employee, dismissal.

Sign-in options

Sign in

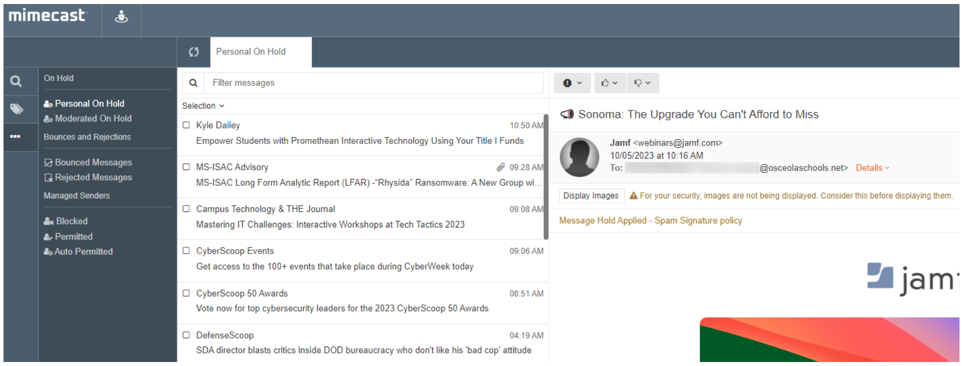
https://fs.osceola.k12.fl.us

Username [redacted]

Password ••••••••••••

Sign in Cancel

This will successfully log you in to the Mimecast Personal Portal where you can click on the Portal App which will take you to view your held messages. See below:



Kyle Dailey 10:50 AM
Empower Students with Promethean Interactive Technology Using Your Title I Funds

MS-ISAC Advisory 09:28 AM
MS-ISAC Long Form Analytic Report (LFAR) -"Rhysida" Ransomware: A New Group wi...

Campus Technology & THE Journal 09:08 AM
Mastering IT Challenges: Interactive Workshops at Tech Tactics 2023

CyberScoop Events 09:06 AM
Get access to the 100+ events that take place during CyberWeek today

CyberScoop 50 Awards 08:51 AM
Vote now for top cybersecurity leaders for the 2023 CyberScoop 50 Awards

DefenseScoop 04:19 AM
SDA director blasts critics inside DOD bureaucracy who don't like his 'bad cop' attitude

Sonoma: The Upgrade You Can't Afford to Miss

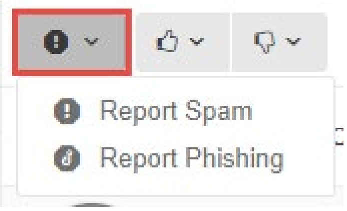
Jamf <webinars@jamf.com>
10/05/2023 at 10:16 AM
To: [redacted]@osceolaschools.net> Details

For your security, images are not being displayed. Consider this before displaying them.

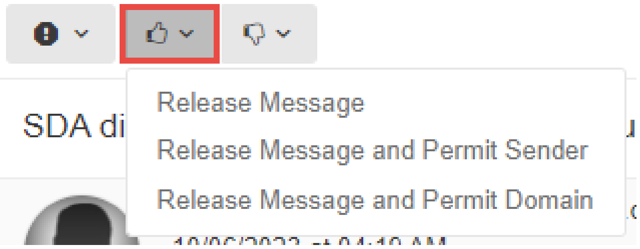
Message Hold Applied - Spam Signature policy

Emails for you to choose to release and permit will be available under "Personal On Hold", where you can select from one of the three options in the message window.

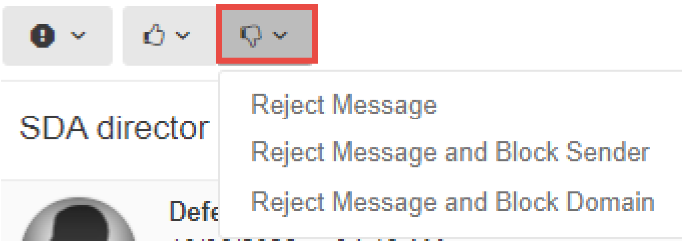
Report Email – From here you can report any message as Spam or Phishing to Mimecast for additional review.



Release Email – From here you can Release Message (future messages from this sender may still be held), Release Message and Permit Sender (this will permit all future emails from this one sender for you) or Release Message and Permit Domain (this will permit all future emails from anyone in the same domain, ex: randomemail.com, to you).

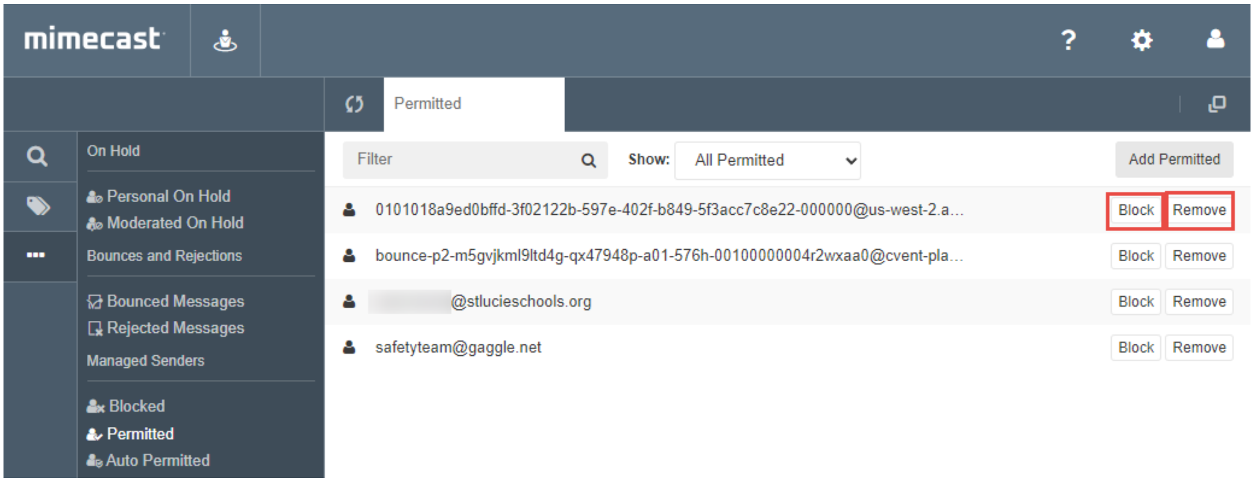

SDA di
Release Message
Release Message and Permit Sender
Release Message and Permit Domain

Reject Email – From here you can Reject Message (future messages from this message will still come in), Reject Message and Block Sender (this will reject the message and block all future emails from this sender for you) or Reject Message and Block Domain (this will block all future emails from anyone in the same domain, ex: randomemail.com, to you).


Reject Message
Reject Message and Block Sender
Reject Message and Block Domain
SDA director
Defe

Also available for you to review are messages that could be on hold but placed in a moderated hold. These messages could be on hold as they didn't pass a security policy in place to protect you and they possibly resemble some form of phishing attack (dangerous URLs/attachments), or they could be impersonating district staff. These will need to be reviewed by the Network Security Team so we can verify if they are dangerous or safe and can be released.

If you accidently block a sender or wish to remove someone from your Allowed Senders list, you may review these under the "Managed Senders" section.



0101018a9ed0bffd-3f02122b-597e-402f-b849-5f3acc7c8e22-000000@us-west-2.a... Block Remove
bounce-p2-m5gvjkml9ltd4g-qx47948p-a01-576h-00100000004r2wxaa0@cvent-pla... Block Remove
[redacted]@stlucieschools.org Block Remove
safetyteam@gaggle.net Block Remove

From here you can modify your Blocked/Permitted entries by either selecting Block or Remove and this will make the appropriate changes for your mailbox.

Snooping

Snooping on District computer systems is a serious security violation. Do not attempt to access information without a legitimate work-related reason. If unintentionally, a new way to access information is identified, it is to be reported to the employee's immediate administrator/supervisor. Watching other users enter information and looking at District information that is not strictly related to the employee's work is prohibited. Obtaining or trying to obtain other users' passwords or using programs that compromise security in any way, are violations of District procedures, as well as violations of state and federal statutes. If snooping is personally observed, it is to be reported to the observer's immediate administrator/supervisor.

Hackers

Hackers are working hard to break into computer systems. They alter and delete files and create havoc for fun or profit. Hackers frequently penetrate computer systems by calling unsuspecting employees representing themselves as a new employee, a District administrator, or another trusted individual. Through a variety of probing questions, they obtain the information necessary for their hacker programs to work.

Do not reveal any information about computer systems in telephone conversations or in any other way, with the exception of calling the Help Desk. If someone requests such information, obtain the name and phone number and promise a response. Report the incident immediately by calling the Help Desk at 407-870-4000 or extension 67000. All employees have a part in protecting District computer systems and information.

Employees are prohibited from using hacker programs and hacker techniques to gain access to District computer systems or using District equipment to hack third party computer systems. Violators will be reported to the local authorities. Hacking is a serious offense. If caught, an employee risks suspension, termination or criminal charges. Employees are to report any security vulnerability identified in the District's network or computer systems to the Help Desk at 407-870-4000 or extension 67000.

SOCIAL NETWORKING

Use of social media websites such as Facebook and TikTok should not be used for communication with students or parents. District provided Outlook Email, Microsoft Teams, Canvas, or Remind accounts are the approved communication options available for staff to communicate with students or parents.

Schools may submit a request in writing to the Community Relations Department for District social media sites. Only the Superintendent or his or her designee may grant approval for additional District social media sites. Refer to School Board Rule, 8.601+, Social Media for more information.

DISTRICT SCHOOL/DEPARTMENT WEBSITES

Employees are not permitted to use free or paid Web hosting services (e.g. GoDaddy, Weebly, etc.) for disseminating information to the public. Each school or department Website is to be hosted on a District server or District approved service. District and school Internet sites are a hosted service, while department and school intranet sites are implemented using Share Point. Teachers interested in having their own webpage should contact their school's webmaster or Community Relations Department for more information.

Refer to School Board Rules, 8.60+, Network Acceptable Use for more information.

U. S. COPYRIGHT LAWS

Copyright Infringement

The District does not own computer software, but rather licenses the right to use software. Accordingly, District licensed software may only be reproduced by authorized District officials in accordance with the terms of the software licensing agreements. Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material is illegal and strictly prohibited. U. S. Copyright laws also apply to Internet resources. Copyright infringement is serious business and the District strictly prohibits any such activity. Contact the Director of Media & Instructional Technology or the local school Media Specialist with questions related to copyright.

Free apps and websites often have licensing and use restrictions and should not be copied or forwarded to others. It is a violation of copyright law to provide a program to a friend without proper licensing. It is not unusual for "free" software to contain a virus.

Each employee is responsible for the software he or she uses. If unsure about school or department software licenses, ask an immediate administrator/supervisor. The school or department bookkeeper will have purchasing records reflecting payment for the number of licensed products currently in use.

Information, images, music, personal streaming services and other types of content found on the Internet are also protected by copyright. Using personal streaming services in the classroom, including but not limited to Netflix, Amazon Prime, Hulu, and Disney+ violates the terms of agreement of the streaming service. It is not permissible to use these types of materials without the permission of the copyright holder. The term "Fair Use" does not imply unlimited use of copyrighted information, images, music, or other types of information without permission of the copyright holder. The school district document “Guidelines for Digital Use” specifies the procedure for showing films and movies in the classroom. Anytime a film is shown for entertainment purposes, the school must obtain a movie license for such purposes, as viewing films and videos for entertainment purposes does not constitute “Fair Use”. The District will, in no way, support any employee charged with a copyright violation.

USING TECHNOLOGY WITH STUDENTS

Internet Safety

IMPORTANT: Any employee including, but not limited to, teachers, paraprofessionals, and extended day staff that supervises students has a responsibility to instruct, supervise, and monitor appropriate usage of the online computer network and access to the Internet. Reference Osceola County School Board rule 8.602+ adopted on December 12, 2023.

Software and Web Tools

The District established a Software and Web Tools Evaluation Committee to review and approve requests for the purchase of new software or web applications/tools, as well as the use of free software and web applications/tools. Many free software and web tools require the creation of student accounts and these requests must be reviewed by the committee. A list of the committee approved software applications and/or web tools can be found on the Media & Instructional Technology website.

The District’s new policy is to re-evaluate approved software and web tools every five years. Employees should always check the approved list at the beginning of every school year to verify an application remains on the approved list.

To protect student privacy, the District has instituted standards for student accounts created by employees for use in the classroom. Employees are to adhere to the following naming conventions for **approved** digital resources that are not automatically uploaded by District staff. All District employees need to comply with Federal laws including the Family Educational Rights and Privacy Act (FERPA) and the Children’s Internet Protection Act (CIPA).

Field Name	Required Information
User Name	49XXXXXXX (x= Seven Digit Student ID)
Password	49MMDD (MM=Birth Month, DD=Birth Day)
First Name	Student's Actual First Name (If more than one student has the same first name, add A, B, C, etc., after the first name)
Last Name	ABC (All students have the same last name)
Date of Birth	10/10/10 (All students have the same birthday)
E-mail Address	District provided student e-mail address

Employee's Cellular Telephones
Employees shall not use personal cellular telephones or other personal communication devices to communicate with students in any way, including but not limited to, texting and instant messaging. Refer to School Board Rule 6.321+ Employee Use of Cellular Telephones.

Exceptions to this policy shall include:

- *When no District cellular telephone or other communication device is reasonably available to the employee, an employee may use a personal cellular telephone or other personal communication device to communicate with a student in an emergency situation in order to ensure the safety of the student. In such emergency situations, the employee shall report this communication to an administrator immediately, and no disciplinary action shall be taken against the employee who acts in good faith. However, the use of such device may not violate School Board Rule 6.84 or any other law or regulation that is intended to prohibit inappropriate conduct or communication with students and/or minors.*

Employees shall not allow students to view any website or other digital content on the employee's personal cellular telephone or other personal communication device. Participation in Federal Programs (e.g. E-Rate) requires content to be filtered for students.

Employees shall not use their personal cellular telephone or other personal communication device to establish connectivity to the Internet (e.g. hotspot) for student access or to circumvent the District filtered network for either personal or student access.

Per Chapter 119, Florida Statutes, if an employee uses a personal cellular telephone or other personal communication device to conduct District business pursuant to an employee's official role and duties, the employee's personal cellular telephone or other *personal communication device may be subject to inspection in response to a public records request or official District or law enforcement investigation.*

Student E-mail Accounts

The District approved student e-mail system is Microsoft's Office365. Students will have e-mail accounts, cloud storage, collaborative spaces, document and video sharing, Minecraft, and online document editing capabilities. Accessible on all devices with Internet access and a web browser, Office365 will provide students with communication and productivity services they need to be career and college ready. For additional information, contact the Director of Media & Instructional Technology.

Technology Support

The school assigned computer tech and school Media Specialist are available to assist school staff on a variety of technical concerns and access to digital resources. The "Greenshirts" from the Media and Instructional Technology Department provide extra technology support for teachers. Additionally, the Technology Services Department provides technical support for all schools and departments.

District departments can create a ticket in Incident IQ or contact the Help Desk at 407-870-4000 or extension 67000.

ELECTRONIC COMMUNICATIONS

E-mail

The same standards of decorum, respect, and professionalism that guide face-to-face interactions apply to the use of e-mail. The District's Network Acceptable Use Policy, School Board Rules, 8.60+, outlines expectations of employees regarding the use of e-mail.

District business conducted by e-mail must be done using the e-mail account the Districtprovides. Forwarding of District business related e-mail messages to your personal e-mail account is **prohibited.**

Incidental or occasional use of e-mail for personal reasons is permitted but should not interfere or conflict with District business. However, only District personnel, active students, and other authorized users approved by the Chief Information Officer or his/her designee are allowed access to the District's e-mail system. The following e-mail activity is prohibited, and in some cases illegal:

- Accessing, or attempting to access, another user's e-mail account
- Obtaining, or distributing another user's e-mail account password

- Using e-mail to harass, discriminate, or make defamatory comments
- Using e-mail to make off-color jokes, or send inappropriate e-mail to third parties or other District employees
- Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes

Employees are required to report inappropriate use of e-mail to their immediate administrator/supervisor.

Dangers and Pitfalls of E-mail

If a message is inappropriate for a memorandum on District letterhead, do not use e-mail.

E-mail is not the only form of communication available to employees. If the communication contains something confidential or sensitive, there are other ways to relay the message. It is still good practice to use the phone, or stop by someone's office and talk face-to-face.

Virus Control

The most widespread means of a virus attack is through e-mail. It is important that employees exercise caution. Do not forward or open web links or attachments that are unsolicited or from unknown sources. The District screens inbound and outbound e-mail messages for viruses, and places restrictions on the ability to open certain file types commonly used in virus attacks.

A web link may not be legitimate, and may be "phishing" to verify e-mail addresses to a spammer or seek personal information that can be used for identity theft.

E-mail Signatures

The District's Network Acceptable Use Policy, School Board Rules, 8.60+, establishes the format for e-mail signatures. Employees shall use the following format for e-mail signatures:

1. Employee's Legal Name
2. Job Title (s)
3. Award or Honor Designation (e.g. Teacher of the Year, etc.)
4. School or Department
    a. The official school or department logo may also be included if its memory size does not interfere with the inclusion of all other required elements of the District format in Paragraph IX.A. of this policy.
5. Work Address

6. Work Phone Number(s)
7. Work Fax Number
8. Work E-mail Address
9. District Mission Statement
    a. "Inspiring all learners to reach their highest potential as responsible, productive citizens."
10. District Vision Statement
    a. "The Osceola School District will work in partnership with families and the community to ensure all learners develop the essential knowledge and skills of successful, future-ready graduates."
11. Legal Statement regarding Florida Public Records Law
    a. "The information contained in this e-mail message is intended solely for the recipient(s) and may contain privileged information. Altering the contents of this message is prohibited. This information is the same as any written document, may be subject to all rules governing public information according to Florida law, and shall not be altered in any manner that misrepresents the activities of the School District of Osceola County, Florida [FSC I.24; FS Chapter 119]. If you received this message in error or are not the named recipient, please notify the sender, and delete this message."

No other information is permitted in e-mail signatures (e.g., personal quotations). The employee's e-mail signature must use a font that is compliant with federal guidelines for the Americans with Disabilities Act. Fonts include, but are not limited to, Arial, Calibri, and Times New Roman; minimum 12 point size font; and high contrast colors such as black on a white background.

<u>Student Information in E-mail</u>

The exchange of student information is regulated by state and federal law. It is illegal to send personally identifiable student information to parties that have no legitimate educational interest in the student.

District policy allows for the exchange of individual student information only between District employees using the District assigned e-mail system. Messages sent to external Internet e-mail addresses can potentially be intercepted, or mistakenly sent to wrong addresses. In these cases, e-mail must NOT contain identifiable student information. The employee may substitute a student's initials for an identifiable name. This restriction applies to all Internet e-mail, including parents, and outside counseling agencies.

Spam

Employees using District e-mail to send unsolicited messages or files, considered electronic junk mail, to individuals, groups, or organizations with the intent to cause harm or damage to the intended receiver are violating the policies of the District and engaging in illegal activities. Violators will be prosecuted to the fullest extent of the law.

Passwords

Effective July 10, 2024, the minimum character requirement for all employee passwords has been increased from 8 characters to 14 characters. The next time your password expires following this date, the new password must meet the new 14 character minimum requirement. Passwords should contain a mix of uppercase letters, lowercase letters, and numbers or special characters. Passwords cannot contain common words, phrases or personal information and must be changed every 90 days.   Employees shall not share passwords or set up any District account for automatic log in.

The default password assigned to new accounts is widely known. New employees must change the default Active Directory password before accessing their district provided e-mail account.

Employees are responsible for all e-mails sent from their District provided e-mail account.

Mobile Devices

Florida Public Record laws consider e-mail documents concerning District business to be public record. It is important to remember this when using mobile devices such as cell phones, Smartphones, and other devices to send e-mail messages that contain content related to District business. Conducting District business on personal devices opens those devices to searches in cases of public records requests or subpoenas.

Archiving

Effective May 31, 2016, District e-mail is archived for all users. All messages received and/or sent are stored on an archive server for three years. Any records requiring retention longer than the automatic three-year time period shall be maintained and accessible in compliance with the Florida Public Records law and the District Records Management Manual. E-mail shall not be used as the retention site for School District business records. Employees are ultimately responsible for managing their own e-mail and maintaining required records.

Account Privacy

The District’s Network Acceptable Use Policy states that minor personal use of e-mail is permitted. However, employees shall not expect privacy because the e-mail system is used to conduct the business of the school District. Contents of an e-mail account may be monitored and/or retrieved for legitimate reasons by authorized personnel. In addition, the contents of employee mailboxes are subject to public records requests, as well as subpoenas and requests from law enforcement agencies.

It is recommended that employees use their own personal e-mail accounts, not District resources, for personal messaging.

Help and Tutorials

Users can get assistance through the school’s computer tech and teachers can contact their school’s Greenshirt for help.

PERSONAL DEVICES

Access and Responsibility

The District is not responsible for any personally owned devices. The District reserves the right to log, monitor, examine, and evaluate all usage of its technology resources. If an employee is authorized to access the District network with a personally owned device, the employee’s personally owned device is subject to all District policies and procedures to include audits, physical inspections, computer forensic inspections and legal seizures, when applicable. Abuse of network resources or network security violations will be cause for disciplinary action, up to and including termination and criminal charges.

Employee Guest Wireless Network

Employee permitted devices include personal cellular telephones, personal laptops, tablets, iPads, iPods, electronic readers and other devices approved by the Chief Information Officer, or his/her designee. Employees accessing the guest wireless network are to have up-to-date antivirus software on personal devices.

Employees may choose to connect, pursuant to their duties, personal cellular telephones or other personal communication devices to the District's guest wireless network. Employees' personal devices connected to the District's guest network may be subject to a public records request or official District or law enforcement investigation. Employees are expected to comply with the District Network Acceptable Use Policy, School Board Rules, and procedures outlined in the Employee Technology Awareness and Security Handbook.

Student Guest Wireless Network

In 2021, the District became a 1:1 learning environment. All students in grades PreK-2 have an assigned iPad and students in grades 2-12 have an assigned computer laptop.

Starting in August 2022, students may choose to connect cellular telephones to the guest network. Personal devices such as laptops, tablets, iPads, iPods, or electronic readers are no longer permitted on the guest network. Teachers can make recommendations to students but are not permitted to require student owned personal cellular telephones to have specific apps/software. Students are expected to comply with the District Network Acceptable Use policy, Student Internet and Network Use Procedures (FC-820-2259), and Code of Student Conduct.

Failure to adhere to this policy may result in disciplinary action up to and including termination of the employee or expulsion in the case of a student.

Employee’s Personal Devices and Students

Under no circumstances should an employee permit students to view unfiltered content on an employee’s personal device not connected to the network (e.g. placing your personal cell phone under a document camera to display content and circumventing the District’s filtering system). Participation in Federal Programs (e.g. E-Rate) requires content to be filtered for students.

Guest Wireless Network - Visitors

External devices owned by sales representatives, consultants, and/or other visiting professionals are permitted to connect to the District’s guest wireless network. Contact your school’s computer tech or the Help Desk for assistance. The school's computer tech or other administrative staff can create a temporary account for authorized visitors to use the guest wireless network.

Confidential Information

Access to confidential information and files may be restricted to protect the security of the District and its administrative records, rights of privacy, and confidentiality. Users who are provided access to such restricted information and files shall exercise the utmost care to prevent unauthorized persons from gaining access to such information and files, and to maintain the confidentiality of such information.

Employees must follow District policies and federal statutes (FERPA) to protect confidential student information, and access only the student information in which he/she has a “legitimate educational interest.”

Using personal external mobile devices such as jump drives, external USB hard drives to transfer confidential information about students, personnel, and /or District business files is PROHIBITED. Transferring any confidential information to other computers or devices outside the District network is prohibited.

Disciplinary Actions

If an employee violates any of the conditions of this District policy related to technology, his/her access may be limited or terminated and future access may be denied. Abuse of network resources or network security violations will be cause for disciplinary action, up to and including termination and criminal charges.

PURCHASING GUIDELINES

Purchases of Computer Software and Hardware

All employees must adhere to District procedures and existing vendor bids/contracts when purchasing computer software and hardware. The Purchasing Department has established procedures to ensure cost-effective purchasing practices to ensure compatibility with existing District computer software and hardware.

The District has a Software and Web Tools Evaluation Committee to review and approve requests for the purchase of new software or web applications/tools. Updated monthly, a list of approved software can be found on the Media and Instructional Technology website https://www.osceolaschools.net/domain/146 under “Software Web Tools or iPad Selection.”

All authorized P-Card holders must follow current P-Card procedures. Contact the school/department bookkeeper or the Purchasing Department for more information.

LEGAL INFORMATION

Privacy

Data stored on computers, transmission of data between individuals, communications on the Internet, and e-mail may be subject to public records requests. The District reserves the right, without prior notice, to access, disclose, use, or remove both business and personal computer communications, and information for legitimate business and legal purposes.

Audits may be performed on District computers in accordance with District procedures. The District will investigate complaints about inappropriate images on computers, e-mail, or other inappropriate conduct. The District may monitor Internet activity to see what sites are frequented, duration of time spent, files downloaded, and information exchanged.

It is the District's fiduciary responsibility to:

- Establish and enforce procedures to help prevent the violation of personal rights and illegal acts
- Reduce the risk of liability and business interruption to the District
- Maintain a professional work environment

Lawsuits and Subpoenas

District computers, like any other District property, are subject to subpoenas. This means that prosecutors and plaintiffs' attorneys may access District computers, and look at information to gather evidence in a complaint. Do not remove any information from a computer to hinder an investigation of any kind. **Even if the information is exempt from disclosure, and eligible for destruction, you must retain it for at least 30 days after requested.**

Employee's Responsibility to Report Violations

Employees are required to report violations or suspected violations of computer security procedures.

Activities that should immediately be reported to an administrator/supervisor include:

- Attempts to circumvent established computer security systems
- Use, or suspected use, of virus, Trojan horse, or hacker programs
- Obtaining, or trying to obtain, another user's password
- Using the computer to make harassing or defamatory comments or to, in any way, create a hostile work environment
- Using the computer to communicate inappropriate or sexually explicit messages, images, videos, or jokes that may be considered offensive by others
- Illegal activity of any kind

Computer security procedure violations will be investigated. Noncompliance with the District's computer security procedure may result in discipline up to, and including, termination and criminal charges. Employees that report violations, or suspected violations, of District policies and/or procedures will be protected from termination, discrimination, harassment, and any other form of retaliation.

If a computer security vulnerability is identified, employees are required to report it immediately. Call the Help Desk at 407-870-4000 or extension 67000.