Policy No. 401.14

EMPLOYEE USE OF CELL PHONES

The use of cell phones and other communication devices may be appropriate to provide for the effective and efficient operation of the school district and to help ensure the safety and security of people and property while on school district property or engaged in school sponsored activities.

Employees may possess and use cell phones during the school day as outlined in this policy and as provided in the administrative regulation developed by the superintendent. Employees should not use cell phones for personal business while on-duty, including staff development times, parent-teacher conferences, etc., except in the case of an emergency or during prep time or break/lunch times. Employees, except for bus drivers, see below, are prohibited from using cell phones while driving except in the case of an emergency and any such use must comply with applicable state and federal law and district policies and regulations.

Cell phones are not to be used for conversations involving confidential student or employee information.

Employees are prohibited from using a cell phone while driving during work duties, unless in the case of an emergency, the vehicle should be in a complete stop with the gear in park.

School bus drivers are prohibited from using any communication device while operating the bus except in the case of an emergency, or to call for assistance, after the vehicle has been stopped. Any such use must comply with applicable state and federal law and district policies and regulations.

Cell Phone Allowance

Certain positions within the district may require the regular use of cell phones to conduct district business. These employees may purchase and/or maintain cell phones and related equipment, at their own expense, to make themselves accessible to the district and to conduct district business more efficiently. The superintendent has discretion to determine which district positions qualify for a cell phone allowance. The monthly cell phone allowance amount shall be established by the superintendent and/or the board. Employees who utilize their personal cell phones shall do so in accordance with this policy and accompanying procedures. The cell phone allowance is neither permanent nor guaranteed. The district reserves the right to rescind the allowance at any time for a violation of district policy or regulation or for any other reason.

Employees violating the policy will be subject to discipline, up to and including discharge. It is the responsibility of the superintendent to develop administrative regulations regarding this policy.

Approved July 18, 2019 Reviewed 6/20/19 Revised _____

Code No. 401.13

Staff Technology, Social Media and Other Electronic Communication

Computers are a powerful and valuable education and research tool and, as such, are an important part of the instructional program. In addition, the school district depends upon computers as an integral part of administering and managing the schools' resources, including the compilation of data and recordkeeping for personnel, students, finances, supplies and materials. This policy outlines the board's expectations in regard to these different aspects of the school district's computer resources. Employees must conduct themselves in a manner that does not disrupt from or disrupt the educational process and failure to do so will result in discipline, up to and including discharge.

General Provisions

The superintendent is responsible for designating a technology coordinator/director who will oversee the use of school district computer resources. The technology coordinator/director will prepare in-service programs for the training and development of school district staff in computer skills, appropriate use of computers and for the incorporation of computer use in subject areas.

The superintendent, working with appropriate staff, shall establish regulations governing the use and security of the school district's computer resources. The school district will make every reasonable effort to maintain the security of the system. All users of the school district's computer resources, including students, staff and volunteers, shall comply with this policy and regulation, as well as others impacting the use of school equipment and facilities. Failure to comply may result in disciplinary action, up to and including discharge, as well as suspension and/or revocation of computer access privileges.

Usage of the school district's computer resources is a privilege, not a right, and that use entails responsibility. All information on the school district's computer system is considered a public record. Whether there is an exception to keep some narrow, specific *content* within the information confidential is determined on a case by case basis. Therefore, users of the school district's computer network must not expect, nor does the school district guarantee, privacy for e-mail or use of the school district's computer network including web sites visited. The school district reserves the right to access and view any material stored on school district equipment or any material used in conjunction with the school district's computer network.

The superintendent, working with the appropriate staff, shall establish procedures governing management of computer records in order to exercise appropriate control over computer records, including financial, personnel and student information. The procedures will address:

- passwords,
- system administration,
- separation of duties,
- remote access,
- data back-up (including archiving of e-mail),
- record retention, and
- disaster recovery plans.

Staff Technology

All of the District's automated systems, including electronic mail, voice mail, Internet access and electronic storage systems, are District property and are not confidential. **The District has the right to access, review, copy, modify, and delete any information transmitted through or stored in the system, including e-mail messages.** Files containing personal information or business of an employee are treated no differently than the District's files, and the employee has no expectation of privacy in such materials.

COMPUTERS OWNED BY THE DISTRICT

Whether being used in the District or in another location:

- Only authorized employees, authorized students, or persons authorized by the administration may use the computer as use by others puts District assets and records in jeopardy. You are not to allow unauthorized persons access to District computer equipment, whether by allowing use of the computer or by viewing the contents of the computer.
- Only software approved by the District shall be loaded on the computer.
- Passwords need to be kept in a discreet location.

E-MAIL USAGE POLICY

Use of e-mail to engage in any communication in violation of District policies including transmission of defamatory, obscene, profane, offensive, or harassing messages, or messages that disclose personal information without authorization, is strictly prohibited.

Use caution in addressing messages to ensure that new messages are not inadvertently sent to the wrong party. This is critical because of the sensitive nature of the documents we often may be asked to e-mail. Always double check that the address you are using is correct and current.

E-mail and other electronic communications systems can be useful tools, permitting rapid and efficient communication with a large audience. This same strength can be a weakness, as a hastily written note may be subject to misinterpretation in the future, when the context is not so clear. This is particularly true when your message is subject to being forwarded, rerouted, or saved by others. For this reason, when sending electronic messages, you should keep the following text in mind: "Would I be concerned if I had to read this message out loud, under oath, as a witness in a courtroom proceeding?" If that possibility does not unduly concern you, then your message is probably acceptable.

Use of another user's name/account to access e-mail or the Internet is strictly prohibited.

INTERNET USAGE

Internet resources may be used only for purposes that effectively support the District's goals and objectives or for the non-business purposes that are approved by the administration. The District has the ability and reserves the right to review records of use of the World Wide Web.

The District will not be responsible for maintaining or payment of personal Internet accounts. You must respect all copyright and license agreements regarding software or publications they access from the Internet. The District will not condone violations of copyright laws and licenses,

and you will be personally liable for any fines or sanctions caused by any license or copyright infringement.

Social Networking or Other External Web Sites

The Collins-Maxwell Community School District recognizes and encourages the use of social media as an educational and communication tool. The District also recognizes that the lines between educational and personal use of social media can be confusing. In all instances it is important that employees and students conduct themselves in such a way that their educational or personal use of social media does not adversely affect their status with the District. Just as the District encourages the use of social media, the District also encourages employees and students to use good and sound practices when using social media.

The purpose of this policy is to establish protocols for the use of social media by employees and students as well as to outline expectations for its use. These protocols are in place regardless of whether access to any social media is through a District-owned computer or other electronic device.

For purposes of this policy, "social media" is any form of online publication or presence that allows interactive communication, including, but not limited to, social networking websites such as Facebook, YouTube, Twitter, Instagram, or similar sites now or in the future. In addition, personal web pages or blogs, educational networking sites, email, texting, instant messaging, and other electronic communication fall under this policy as well.

For purposes of this policy any website, other than the school district web site or school-school district sanctioned web sites, are considered external web sites. Employees shall not post confidential or proprietary information, including photographic images, about the school district, its employees, students, agents or others on any external web site without consent of the superintendent. The employee shall adhere to all applicable privacy and confidentiality policies adopted by the school district when on external web sites. Employees shall not use the school district logos, images, iconography, etc. on external web sites. Employees shall not use school district time or property on external sites that are not in direct-relation to the employee's job. Employees, students and volunteers need to realize that the Internet is not a closed system and anything posted on an external site may be viewed by others, all over the world. Employees, students and volunteers who don't want school administrators to know their personal information, should refrain from exposing it on the Internet. Employees should not connect with students via external web sites without consent of the superintendent. Employees, who would like to start a social media site for school district sanctioned activities, should contact the superintendent.

Expectations for All Use of Social Media and Other Electronic Communication:

- Employees and students should understand and abide by the social media site's policies and terms of use.
- Employees and students should understand that they are personally responsible for the content they post or otherwise publish on social media. Only predetermined staff members are to act as representatives of or spokespersons for the District.
- Employees and students should not post or otherwise publish content that is deemed

defamatory or obscene or which constitutes an incitement to imminent violence or a true threat, or which violates copyright or other intellectual property laws.
- Employees and students should be careful about the type and amount of personal information they provide on social media.

- Employees and students should not post or otherwise publish confidential or protected information about the District, its employees, or students. Disclosure of confidential or protected information may result in liability for invasion of privacy or defamation.
- Employees and students should set and maintain appropriate social networking privacy settings. Be aware that social media sites can change their privacy policies and standards at any time, possibly exposing posts that employees and students believed were private to the public.

Expectations for Educational Use of Social Media and Other Electronic Communication:
- Employees and students accessing social media or other electronic communication through a District-owned computer or other electronic device or network are subject to applicable laws and District policies and rules regarding acceptable use of such District-owned resources, including, but not limited to, the District's Acceptable Use of the Internet policy (see Code No. 401.13a)
- Employees and students accessing social media or other electronic communication at school are subject to District policies and rules regarding appropriate conduct. It is important to remember that infractions prohibiting certain types of communication, such as bullying and harassment, also apply to electronic communication. Behavior that is inappropriate in face-to-face interactions with others at school should be considered inappropriate online.
- Employees may create a social media site for a school, class, or program only with the prior approval of the District Superintendent or designee. No school logos, mascots, photographs of the facilities, or other such graphic representations or images associated with the District may be used without permission.

Expectations for Personal Use of Social Media and Other Electronic Communication:
- Employees should carefully consider the pros and cons, potential difficulties, and additional responsibilities that may be involved if they accept current District students as "friends" or "follow" them on social media. Employees are expected to maintain appropriate professional boundaries in their electronic communications with students.
- Employees should consider whether a particular posting on social media or other electronic communication puts their professional reputation and effectiveness as a District employee at risk.
- Students should consider that their social media or other electronic communication use may result in disruption at school and the school may need to get involved.

Employees and students found to have engaged in inappropriate use of social media or other electronic communication may be subject to disciplinary action by the District, up to and including termination and expulsion. It is the responsibility of the superintendent to develop administrative regulations implementing this policy.

Approved July 18, 2019 Reviewed 6/20/19 Revised _____

Staff Technology Use/Social Networking Regulation

General

The following rules and regulations govern the use of the school district's computer network system, employee access to the Internet, and management of computerized records:

- Employees will be issued a school district e-mail account. Passwords must be changed periodically.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- Employees are expected to review their e-mail regularly throughout the day, and shall reply promptly to inquiries with information that the employee can reasonably be expected to provide.
- Communications with parents and/or students must be made on a school district computer, unless in the case of an emergency, and should be saved and the school district will archive the e-mail records according to procedures developed by the Director of Technology.
- Employees may access the Internet for education-related and/or work-related activities.
- Employees shall refrain from using computer resources for personal use, including access to social networking sites.
- Use of the school district computers and school e-mail address is a public record. Employees cannot have an expectation of privacy in the use of the school district's computers.
- Use of computer resources in ways that violate the acceptable use and conduct regulation, outlined below, will be subject to discipline, up to and including discharge.
- Use of the school district's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Off-site access to the school district computer network will be determined by the superintendent in conjunction with appropriate personnel.
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the school district's network must notify appropriate staff. Any network user identified as a security risk or having a history of violations of school district computer use guidelines may be denied access to the school district's network.

Prohibited Activity and Uses

The following is a list of prohibited activity for all employees concerning use of the school district's computer network. Any violation of these prohibitions may result in discipline, up to and including discharge, or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising, or personal gain.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the school district computer network.
- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material

Staff Technology Use/Social Networking Regulation

- Using the network to receive, transmit or make available to others messages that are racist, sexist, and abusive or harassing to others.
- Use of another's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy school district equipment or materials, data of another user of the school district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network to send anonymous messages or files.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network for sending and/or receiving personal messages
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal disks on the school district's computers and/or network without the permission of the Director of Technology.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

Other Technology Issues

Employees with personal cell phones should not be using the phones for school district business. Employees should contact students and their parents through the school district computer or phone unless in the case of an emergency or with prior consent of the principal. Employees should not release their cell phone number, personal e-mail address, etc. to students or their parents. Employees, who are coaches or sponsors of activities, may create a text list of students and parents in order to communicate more effectively as long as the texts go to all students and the principal is included in the text address list.

SCHOOL EMPLOYEE AND BOARD MEMBER ACCEPTABLE USE POLICY FOR THE INTERNET, LOCAL AREA NETWORK, WORLD WIDE WEB, AND GENERAL TECHNOLOGY USE

Code No. 401.13a

The use of technology in the Collins-Maxwell Community Schools is a privilege extended to those individuals who wish to enhance their learning experiences. The Local Area Network and access to the Internet and World Wide Web are the property of the Collins-Maxwell Community Schools. The "Systems Administrator" and/or building administrators may access files when deemed necessary for compliance with the Acceptable Use Policy. All users must work within the guidelines (Acceptable Use Policies) of the Collins-Maxwell Community Schools. The authority for appropriate use of electronic Internet resources is delegated to licensed employees. Instruction in the proper use of the Internet system will be available to employees who will then provide similar instruction to their students. Employees and board members are expected to practice appropriate use of the Internet, and violations may result in disciplinary action up to and including termination of employment.

1. All use of the District's computer, network, Internet, and World Wide Web must be in support of education and research, and must be consistent with the Acceptable Use Policy of the District. The use of social networking sites is restricted to school business.
2. Network accounts are to be used ONLY by the authorized owners of the accounts, for authorized purposes. Users must NOT give their account names and/or passwords to anyone else. Users who allow others to use their account names and/or passwords may lose the privilege to use the District's computer, LAN, Internet, and/or World Wide Web.
3. Users shall not seek or modify data or passwords belonging to other users, or misrepresent themselves to other users on the District's Computers, LAN, Internet, or World Wide Web. Reading or using another person's files is considered electronic "breaking and entering" and will not be tolerated.
4. All communications and information accessible via the LAN, Internet, and World Wide Web should be assumed to be public property for educational use of the user. The Systems Administrator and/or instructor retain the right to view and/or remove information located on, the District's computers or procured by, the LAN, Internet, or World Wide Web.
5. No use of the District's computers, LAN, Internet, or World Wide Web shall serve to disrupt the use of the network by others; no hardware or software shall be modified, abused, or destroyed.
6. Use of the District's computers, LAN, Internet, or World Wide Web to develop or use programs or activities that harass other users, and/or the infiltration of a computer or computing system and/or damaging the software components of a computer or computing system is prohibited. Computer "hacking" and other unlawful activities will not be tolerated.
7. Harassment, discriminatory remarks and/or any other disrespectful behavior are prohibited on the District's computers, LAN, Internet, or World Wide Web.
8. The use of the District's computers, LAN, Internet, or World Wide Web to access or process materials that are threatening, prejudicial, obscene, abusive, demeaning, racially offensive, profane, illegal, promote substance use, contain child pornography, harmful to minors, other inappropriate files, or files dangerous to the integrity of the LAN, Internet, or World Wide Web is prohibited.
9. The District's computers, LAN, Internet, or World Wide Web will not be used for the use, disclosure, or dissemination of non-educational personal information regarding minors.
10. The installation of ANY non-school-owned hardware or licensed software on the district network or school-owned computers is prohibited.
11. The District is not responsible for employees' mistakes or negligence, costs incurred by employees for non-school purposes, or the accuracy or quality of information found on the Internet.

I, the undersigned have read, understand, and agree to abide by the Acceptable Use Policies of the Collins-Maxwell Community School's Local Area Network and access to the Internet and World Wide Web.

User Signature_____ Date_____

Approved: 7/18/2019 Reviewed: 6/20/2019 Revised: