*The purpose of this document is to communicate Clayton County Public Schools Board of Education policies to ensure efficient, effective and safe use of all CCPS's digital resources. CCPS provides powerful resources to enhance the educational experience of its students and educators. CCPS employees must adhere to important rules and guidelines to ensure the safety of our infrastructure and students. CCPS monitors Internet traffic to ensure optimal use of digital resources. The following are Clayton County Public Schools Board of Education policies that govern acceptable behavior when using any and all CCPS digital resources. Failure to follow any of these policies may result in confiscation of CCPS's resources, suspension of Internet and network access, and may lead to additional action being taken by the Department of Human Resources.*

1. E-Mail

The CCPS e-mail system is designed to provide electronic communication and use of related resources. Employees or students with e-mail access shall adhere to the following protocols:

1.1 E-mail accounts are provided for employees, students, and approved contractors only.

1.2 E-mail accounts are provided for professional and academic purposes only. E-mail accounts should not be used for personal gain, personal business activities or to solicit for non-school system business; broadcasting of unsolicited messages is prohibited. (i.e., advertising, chain mail, political propaganda).

1.3 Employees and students should not use personal e-mail accounts for CCPS related communications.

1.4 All electronic communication created, sent, or received via CCPS e-mail system or on an electronic device owned or leased by CCPS is the property of CCPS. Employees and students shall not have any expectation of privacy regarding this information. The Board reserves the right, as needed, to access, read, review, monitor and copy all messages and files on its computer system without notice. When deemed necessary, CCPS reserves the right to disclose text, video, audio or image files to law enforcement agencies without the employee's or student's consent.

1.5 Employees and students shall use caution to ensure that the correct e-mail address is used for the intended recipient.

1.6 Alternate Internet Service Providers (ISP) or anonymous connections to Board internal network are not permitted unless expressly authorized by CCPS and properly protected by a firewall or other appropriate security device(s).

1.7 Only authorized administrative personnel are permitted to access another user's e-mail without consent. Users may not deliberately disrupt email services or perform activities that interfere with the use of email by CCPS users.

1.8 Employees and students shall exercise sound judgment when distributing messages. Student related messages should be guarded and protected. Employees and students must abide by copyright laws, ethics rules and applicable state and federal laws.

1.9 E-mail messages should only contain professional and appropriate language. Employees and students shall not send abusive, harassing, intimidating, threatening, discriminatory, or otherwise offensive messages.

1.10 Spam messages, and messages containing malware, inappropriate graphics, executable programs, and/or chain letters shall be deleted.

1.11 E-mail access for retiring CCPS employees or employees leaving the school system will be disabled and/or deleted on the last day of employment.

1.12 Access to e-mail accounts under investigation shall be restricted without notice.

1.13 While CCPS encourages respect for the rights and sensibilities of others, it cannot protect individuals against the existence or receipt of materials that may be offensive to them. Those who make use of electronic communications may encounter or be recipients of material that they might find offensive or annoying. In such cases where materials are received, the users shall delete the non-school system business related content. CCPS is not responsible for the views expressed by individual users via web pages, electronic mail or other on-line communications.

***1.14 Phishing is a method of spam email that attempts to persuade the user into disclosing sensitive information such as network username and password. Please be advised that this type of email does not originate from the Technology Department. The Department of Technology will NEVER ask for your username and password via email. Disclosing or compromising your network username and password is significant and can negatively affect the entire email system.***

1.15 CCPS provides access to its email via a web browser. If you are using a device other than the device provided by CCPS, it is imperative that appropriate security software (enterprise anti-virus and anti-spyware) is loaded on the device. Please consult the Department of Technology for additional information if needed.

1.16 Email users must keep their attachments within the prescribed size limits set by the Department of Technology.

1.17 Privacy. Users do not have a personal privacy right as it relates to CCPS email system or on any electronic device owned or leased by CCPS. CCPS may at time and without prior notice, monitor and review email by users or electronic information stored, received or sent from a CCPS electronic device.

1.18 Users may not send mail to more than 150 addresses at a time. Mail should be sent to a targeted user or group. CCPS email resources may not be used for personal gain or enterprise. Examples include, but are not limited to, political campaigning and business solicitations. Users may not create, forward or reply to chain letters or similar email.

2. Network

2.1 Personal Responsibility: By accepting an account password, related information, and accessing CCPS network, intranet or Internet system, all employees and students agree to adhere to CCPS policies regarding their use. Employees and students should report misuse or policy violation(s) to administration or the Department of Technology.

2.2 Permitted Use and Terms: Use of CCPS network and the Internet is a privilege, not a right. Use of network, intranet and Internet access extends throughout an employee's term of employment and student's enrollment term, providing the employee does not violate CCPS policy.

2.3 Availability and Access: The Chief Technology Officer or designee at his/her discretion has the right to suspend access at any time, without notice for possible CCPS policy violations, security or administrative concerns. The Chief Technology Officer shall have the right to suspend network access at any time, without notice, for technical reasons or possible violation of state and federal laws.

- Network access for retiring CCPS employees or employees leaving the school system will be disabled and/or deleted on the last day of employment.
- Student information system access for retiring CCPS employees or employees leaving the school system will be disabled and/or deleted on the last day of employment.
- Access to network accounts under investigation will be restricted without notice until authorized by the Chief Technology Officer or designee.

2.4 Privacy: Network and Internet access is provided as a tool for school system related business. CCPS reserves the right to monitor, inspect, copy, review, and store at any time, without prior notice, any and all usage of the network and the Internet. This includes, but is not limited to, all materials, files, information, software, communications, and other content transmitted, received, or stored in connection with this usage. All such information, content, and files are the property of CCPS. ***No employee or student should have an expectation of privacy regarding such information.***

2.5 Downloaded Files: Employees and students are reminded that information obtained from the Internet or externally connected device is not always reliable and should be verified for accuracy before use. Any files downloaded from the Internet must be scanned with school system virus detection software before being opened. All CCPS related files should be stored on approved online or internal resources.

2.6 Confidential Information: Employees may have access to staff or student information that is considered confidential as related to their job responsibilities. Employees may use e-mail to communicate confidential information internally to those with a need to know. Such e-mail shall be marked "Confidential". For purposes of this policy, confidential information is defined as:

- Procedures for computer access and passwords of CCPS users, program manuals, user manuals, or other documentation, screen, file, or database layouts, systems flowcharts, and all documentation normally related to the design or implementation of any computer programs developed by CCPS relating to computer programs or systems installed for internal use.
- Lists of information about personnel seeking employment with or who are employed by CCPS.

- Information relating to CCPS research, development, purchasing and marketing.
- Transmission of information that is confidential under CCPS policy, state or federal law or regulations.

2.7 All CCPS users (staff and students) should store all education related data on the provided G Suite platform (cloud storage). All CCPS users are responsible for protecting their data by safeguarding network login credentials. This storage is for work related data only and not for personal files. Applications or programs should not be installed or stored in this location. Files that do not meet the acceptable criteria may be deleted without notification by the Department of Technology.

2.8 Network storage for retiring CCPS employees or employees leaving the school system will be disabled and/or deleted on the last day of employment.

2.9 Unauthorized devices such as wireless access points, wireless hotspots, hubs, or routers are considered rogue devices and may not be used. Such devices may interfere with the CCPS network WAN/LAN. Additionally, users should not plug in any network cables without consent from the Department of Technology.

2.10 The Department of Technology only allows connecting personal devices, i.e., iPhones, iPads, Android smartphones, to the CCPSEdNet or wireless network. The CCPSEdNet wireless network is designed to be separate from the CCPS "secure" network.

2.11 Confidential or sensitive data (student data, Social Security numbers, employee data) belonging to CCPS must not be copied to external storage devices.

3. Software

3.1 Software piracy is both a crime and a violation of CCPS Electronic Communications Policy.

3.2 Employees shall use software strictly in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyrighted software, except for backup and archival purposes by designated administrative personnel, is a violation of copyright law.

3.3 CCPS does not condone, and prohibits, the unauthorized duplication of software. Employees illegally reproducing software shall be subject to disciplinary action. Employees illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment.

3.4 Any employee who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to CCPS, or who places or uses unauthorized software on CCPS premises or equipment, shall be subject to disciplinary action.

3.5 Employees shall not install personal software on CCPS computers.

3.6 Employees shall not copy software from CCPS computer system for installation on home or other computers without prior written authorization from the Department of Technology.

3.7 In unique cases that require an employee to use software at home CCPS will purchase an additional copy or license. Any employee issued additional copy(s) of software for home use acknowledges that such additional copy(s) or license(s) purchased for home use are the property of the CCPS. Employees who are required to use software at home shall contact the Department of Technology or appropriate department that maintains the license to determine if appropriate for home use.

3.8 Employees who suspect or become aware of software misuse shall notify school administration or the Department of Technology.

3.9 No technology software purchases can be made except through CCPS purchasing procedures. The Department of Technology shall be sent a "Request for Approval" form prior to purchase.

3.10 Freeware, third-party software, or any other type of software, obtained, downloaded or purchased is prohibited from being loaded on any CCPS system without the permission of the Department of Technology. This includes, but is not limited to: screensavers, games, weather software, flash or Java cartoons/games/modules, FTP software, remote control software, keyloggers, sniffers, music players, file sharing applications or any other software or component that has the potential to modify the system from its standard CCPS operating system configuration.

4. Hardware

4.1 The computer (laptops, notebooks, desktops, printers, smart devices, etc.) and peripherals issued to a CCPS employee or student are the property of CCPS and are for employee and/or student use only. The computer and peripherals issued to a CCPS employee or student are to be returned immediately if he/she is no longer employed or enrolled by CCPS.

4.2 The computer and network resources are intended for CCPS related purposes and performance of job/classroom duties. The technology acceptable-use policy applies to both work and home use of resources.

4.3 The user is responsible for all technology equipment issued by CCPS. Technology equipment should be locked and safely stored away when not in use.

4.4 Users should promptly report stolen equipment to the Technology Department. In the event of loss or damage, CCPS reserves the right to charge for replacement equipment or not to issue a replacement computer or peripheral. The student and parent/guardian will be responsible for the replacement cost if the device is lost or is damaged because of intentional misuse.

4.5 Configuration and Software. No Modifications or configuration changes are to be made to the computer except upon instruction by the Department of Technology. No software is to be installed on the computer except upon approval by the Department of Technology. Expressly prohibited are peer-to-peer networks such as Psiphon, BitTorrent or any software installed with the sole purpose of bypassing CCPS's security policies.

4.6 Devices issued by the Department of Technology are to be used as specified by the signed user agreement form prior to receiving the device. The Technology Department will not support these devices for any other purpose.

4.7 Student Access. Students are not allowed to use the laptops that have been issued to educators. Educators should use CCPS issued laptops to conduct business. Laptops should be locked when not in use and should not be given to students to perform class work. Students should never be given access to gradebook or any other student data records.

5. Passwords

5.1 School system passwords are considered confidential and shall not be released unless directed by the CCPS Department of Technology.

5.2 School system network and e-mail passwords are initially assigned by the Technology Department and may be changed without notice.

5.3 Users will not share their user ID and password. If the Department of Technology personnel must sign on to a user's account, and the password is not known, then the password will be reset to the system authorized password.

5.4 Employee/Student email and network passwords will be changed periodically on a schedule approved by the Department of Technology.

5.5 Passwords should be memorized. User ID(s) or password(s) should be secured including those kept on mobile devices.

5.6 Users should ensure that they are not being watched before entering a User ID or password. Users are responsible for making sure they avoid obvious "shoulder surfing" by students or other staff.

5.7 Before using the User ID and password on a non CCPS computer, the user should make sure the computer is well protected, free of malware or other software that might allow for a breach of security such as keystroke loggers.

5.8 Failed login sessions will be terminated and the account locked out after a specified number of unsuccessful attempts. Account reinstatement is at the discretion of the CCPS Department of Technology.

5.9 Users will not use special programs to login. Special programs include, but are not limited to, batch files, automatic log-in scripts, software macros, terminal function keys or other software.

5.10 A password shall be changed if it is suspected that it has been disclosed to anyone besides the authorized user.

5.11 Users are required to use the CCPS Portal to manage their accounts in case of forgotten passwords or locked out accounts. All CCPS users (staff and students) are responsible for managing their own passwords through the CCPS Portal.

5.12 Passwords and usernames are the property of CCPS and not the user.

6. Network Security

6.1 All desktops, servers, laptops, or at-risk operating systems will have the system default anti-virus software installed and have current virus signatures.

6.2 Users shall not download any files and/or programs from unknown sources.

6.3 Users shall not open suspicious or non-job related attachments or links, even if they were sent by a friend, family member, or co-worker.

6.4 Users shall make every effort to ensure that all externally connected devices are free of both viruses and malware.

6.5 Users shall not download updates, Service Packs, or any software that might modify the current operating system or network environment unless directed by the Department of Technology.

6.6 If a “stand-alone” (non-networked) machine is used, the machine must run the default CCPS anti-virus software installed and have current virus signatures manually applied.

6.7 It is the responsibility of employees and vendors with VPN privileges to ensure that unauthorized users, i.e., family, coworkers and/or friends, are not allowed access to CCPS internal networks.

6.8 Vendors with authorized VPN access shall be asked to sign an agreement form provided by the Department of Technology.

6.9 Dual (split) tunneling is not permitted; only one network connection is allowed.

6.10 By using VPN technology with personal home equipment, a user should understand that their machines are a de facto extension of the CCPS network, and as such are subject to the same rules and regulations that apply to CCPS owned equipment as related to school system job responsibilities.

6.11 Any employee found to have violated this policy may be subject to disciplinary action, up to and including removal of VPN access, removal of CCPS network access and possible termination of employment.

7. Backup and Recovery

7.1 Backup data will be stored in multiple secure locations.

7.2 User email that is deleted, by the user, will only be retained for 30 days.

7.3 E-mail recovery is only available for disaster recovery purposes. Emails are not available 30 days after termination status.

7.4 Fund accounting backups are run on a daily, weekly, monthly and a yearly rotation. Related data is stored in multiple secure locations.

7.5 Production of e-mail pursuant to open records and investigation requests is not possible 30 days after the user deletes the e-mail from their mailbox or user's employment has terminated. For active employees, older

data that has not been deleted is still available for production pursuant to open records requests or other operation of law.

7.6 Any employee of CCPS who creates an electronic document must review said document for content. Once a determination has been made that the document is subject to Public Records law, the employee should then cause the record to be stored according to this policy by either printing or filing a hard copy.

7.7 Employee Data on Local Machine. CCPS is not responsible for lost or corrupted data in the event of a hardware/software failure or user error. It is the responsibility of the user to maintain a backup of his/her critical data on CCPS equipment. All users should us provided G Suite (cloud storage) platform.

8. Internet Resources

8.1 Users will use appropriate language on the Internet.

8.2 Users will not access or transfer inappropriate materials. Internet traffic is monitored and abuses will be reported.

8.3 Users will respect and uphold copyright laws.

8.4 Downloading games, video files, audio files or running streaming media without educational value and without approval from the Department of Technology is prohibited. Streaming media is bandwidth intensive and can negatively affect important Internet based applications if not used properly.

8.5 Internet content filtering is maintained in compliance with the Children's Internet Protection Act regulations. No attempt should be made to circumvent the district's content filtering solution. Contact the Department of Technology should you need access to a site currently blocked by the filter.

9. Web Resources

9.1 School and/or Teacher websites may NOT publish photos on pages without consent from all individuals and their parents/guardians.

9.2 Teachers may not link to their own personal pages to pages associated with CCPS.

9.3 No student email addresses, home addresses or phone numbers shall be on any web pages.

9.4 No marketing or advertising may be done on Teacher or School websites except for Partners in Education.

9.5 Teachers, webmasters and Principals assume all responsibility for all content displayed within the schools' and the teachers' websites.

Employee Name (Print): _____
Employee Signature: _____
Department or School: _____

For technology related help, please contact: http://supportcenter.clayton.k12.ga.us/ or 770-473-2772.