Centreville Public Schools (CPS)
Staff Acceptable Use Agreement

With the growth of technology and use of telecommunications as a work and learning tool, it is prudent to define the rights and responsibilities of individuals using these tools. The following covers use of telecommunications, district issued and/or supported network, hardware, and software. Including consequences for violations of the policy.

For the purposes of this document the following terms and definitions apply:

● Users - any person using CPS computing or network resources including but not limited to faculty, staff, students, volunteers, community members, etc.

● Network - the telecommunications network owned and operated by CPS that allows for the exchange of data between computing devices using either a wired or wireless connection.

● Cloud Services - Any service that CPS utilizes to house district information / data on a server or service off-site outside of the CPS Information Services network.

1.0 - GUIDELINES FOR USING TELECOMMUNICATIONS

The goal of participation in telecommunications is to assist in the collaboration and exchange of information between and among individuals and between CPS and other schools and institutions.

The intent of this policy is to comply with the stated purposes and acceptable use policies of any networks utilized. This acceptable use policy applies to all users accessing any network and equipment at CPS, both on-site and by means of remote connections.

RIGHTS:

● Users have the right to telecommunicate to facilitate personal growth in technology, information gathering skills, and communication skills. Any use of telecommunications for commercial, advertising, for-profit purposes or political lobbying is prohibited. Extensive use of telecommunications for personal and private business is prohibited. Any use of the Internet for product advertisement is prohibited. Any illegal behavior is prohibited. Selling or buying of research projects in order to represent them as one's own is prohibited.

● Users have the conditional right to use any method for accessing information such as: electronic mail (e-mail), Telnet, and File Transfer Protocol (FTP). Users may send school related e-mail to any member on the Internet.

● Users have the conditional right to sign up for LIST Servers on the Internet.

● Users have the conditional right to request newsgroups from the Internet in order to facilitate real-time learning with members on the network.

NOTE - "Conditional right" is defined as a right subject to limitations of hardware or other limitations imposed by school officials. For example, if there is not room on a network to store a 15GB video file, the user will be required to use an alternate means of storage.

● Network storage areas and District issued devices may be treated like school lockers or desks. Administrators may review e-mail, files, device content, and communications to maintain system integrity and ensure that users are using the system responsibly. Administrators may also request access to these types of documents maintained on third- party servers being used for educational purposes. Users should not expect that files will always be private and should always keep school related accounts separate from any personal accounts. Any accounts used for school related business are subject to FOIA requests.

● The District reserves the right to disable/block specific sites and/or services having a negative effect on the performance of the District's network and information resources and/or to remain compliant with local, state, and federal requirements.

RESPONSIBILITIES:

● Each user is responsible for all material sent electronically. Cyber bullying (hate mail, harassment, discriminatory remarks) and other antisocial behaviors as defined in Board Policies are prohibited. Any violations of the use of telecommunications should be reported to a building administrator.

● Each user assumes personal responsibility and liability, both civil and criminal, for unauthorized or inappropriate use of the Internet.

● Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users.

● Users shall not allow others to use their network account or password. Users shall only access the network with their assigned account and password.

● Users may not use the network to engage in “hacking” or other unlawful activities.

● Users will accept the responsibility of keeping copyrighted material of any kind from entering the network and may not transport any material that is in violation of any State and Federal laws or regulations, or Board policies.

● Users may not use telecommunications to access any pornographic material, inappropriate text files, or files dangerous to the integrity of the school district or any other network. It is the user's responsibility to maintain the integrity of District hosted and/or supported e-mail systems. The user has the responsibility to report all violations of privacy. The user is also responsible for making sure all e-mail sent or received by him/her does not contain pornographic material, inappropriate information, or text encoded files that are potentially dangerous to the integrity of the local area network or other networks. The user is also responsible for reporting any misuse of technology to the proper administrator or other staff immediately.

● Use of the Internet and any information procured from the Internet is at the staff member's own risk. The Board is not responsible for any damage a user suffers, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. The Board is not responsible for the accuracy or quality of information obtained through its services. Information (including text, graphics, audio, video, etc.) from Internet sources used in class should be cited the same as references to printed materials.

● Disclosure, use and/or dissemination of personal identification information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent/guardian or as authorized under the Family Educational Rights and Privacy Act (FERPA).

● Staff members may access social media during work hours only for work related purposes.

● Staff members are prohibited from accessing personal shopping sites and other similar websites during work hours.

2.0 - GUIDELINES FOR THOSE USING HARDWARE AND SOFTWARE

RIGHTS:

Each user has the conditional right to make use of authorized hardware and software found on school grounds in order to facilitate personal academic growth and a greater understanding of the utilization of technology.

RESPONSIBILITIES:

● The user, exercising his/her right to use any hardware and software as an educational resource, shall also accept the responsibility for the preservation and care of that hardware and/or software.

● Only software purchased or authorized by CPS may be stored or installed on district hardware. No software programs may be downloaded off the Internet without prior approval from the CPS Administration and CPS Information Services.

● Only hardware approved by CPS may be physically attached to the district network. Personal hardware (mobile devices) may only be connected to the Public Wifi. It is the user's responsibility to make sure no hardware or software is destroyed, modified, or abused in any way. It is the user's responsibility to make sure that all food and drinks are kept away from all hardware and software. Any damages caused may result in costs levied on the employee for parts and labor.

● It is the user's responsibility to keep malware (i.e. software or content used to disrupt computer operation, gather sensitive information, or gain access to private computer systems) off any school equipment. The user will be held accountable for any deliberate attempts at knowingly installing and/or running a computer virus.

● It is the user's responsibility to keep pornographic material and other inappropriate files off school premises.

● The user is responsible for all files stored or printed under his/her user account without exception. The user is also responsible for ensuring that any device left unattended is secured by a password and/or PIN.

● It is the user's responsibility to keep hardware and software from being removed from school premises without prior consent from an administrator. If the user is assigned a mobile device (laptop, iPad, etc.) they are responsible for physical and data security on and off school premises.

● It is the user's responsibility to obtain approval from the St. Joseph County Information Services prior to removing, relocating, or modifying any hardware or software from its designated location. Mobile devices must be secured while not in use.

3.0 - GUIDELINES FOR THOSE USING PRINTERS

RIGHTS:

Each user has the right to access a printer in order to produce quality documents pertaining to his/her respective topic or interest area and to facilitate personal growth in technology and visual presentation.

RESPONSIBILITIES:

● Each user has the responsibility to monitor all printed documents and be mindful to print only what is needed. It is the user's responsibility to keep images containing pornographic material or material otherwise deemed inappropriate for school use from being printed on any printer or plotter being used on school premises.

● Each user signed onto the network will be responsible for all files printed under his/her user account without exception. Extensive use of district printers for personal and private business is prohibited. Cost per copy can be obtained by referring to the staff handbook under general office information.

4.0 - GUIDELINES FOR THOSE USING SCAN-TO-EMAIL

RIGHTS:

Each user has the right to access a scanner to facilitate personal growth in technology and visual presentation.

RESPONSIBILITIES:

● The user, exercising his/her right to use a scanner as an educational resource, shall also accept the responsibility for the preservation and care of the scanner. Only those users with prior experience or instruction shall be authorized to use a scanner.

● Each user is responsible for all scanned material. It is a user's responsibility to keep images containing pornographic material or material otherwise deemed inappropriate for school use from being scanned and used within the school. All copyrighted materials scanned on district equipment must be accompanied by proper notice of copyright and permission from original author.

5.0 - GUIDELINES FOR THOSE USING TELECOMMUNICATIONS DEVICES AND PERSONAL ELECTRONIC COMMUNICATION DEVICES (PDCs)

RIGHTS:

Each user has the right to access network connections. Network connections may be provided by CPS Information Services, or a commercial carrier, in order to retrieve information from a wide variety of educational resources and to facilitate personal growth in technology, information gathering, and collaboration skills.

RESPONSIBILITIES:

Telecommunication Devices

● The user, by exercising his/her right to use a network connection as an educational resource, shall accept responsibility for its preservation and care.

● Each user is responsible for all files received. It is a user's responsibility to make sure no unauthorized copyrighted materials enter the network.

● It is the user's responsibility to keep pornographic material, inappropriate files, and files known to carry harmful malware off school premises.

Personal Electronic Communication Devices (PCDs)

● A personal electronic communication device is a device owned by a user that emits an audible signal, vibrates, displays a message, or otherwise summons or delivers a communication to the possessor. Examples are: cellular and wireless phones, pagers/beepers, personal digital assistants, smartphones, Wi-Fi enabled or broadband access devices, two-way radios or video broadcasting devices, laptops, portable gaming systems, and other devices that allow a person to record and/or transmit, on either a real time or delayed basis, sound, video or still images, text, or other information.

It is the user's responsibility to:

● View Internet sites that are only allowed at school.

● Respect the privacy of others:

○ Users must receive explicit consent to capture, record, or transmit the words (i.e. audio) and/or images (i.e., pictures/video) of any student, staff member or other person during any classroom activity.

○ Users are prohibited from: sending sexual messages or pictures through text messages ("sexting"), any form of cyber bullying, or any malicious activities.

○ Users are prohibited from using PCDs at any time in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include but are not limited to locker rooms, shower facilities, restrooms, and any other areas where students or others may change clothes or be in any stage or degree of disrobing or changing clothes. The building principal has authority to make determinations as to other specific locations and situations where possession of an ECD is absolutely prohibited.

● Ensure that the use of the PCD does not promote academic dishonesty (i.e., cheating on tests, etc.).

Each user is responsible for their own PCD. Users understand:

● That if devices are loaned to or borrowed and misused by non-owners, device owners are jointly responsible for the misuse or policy violations.

● CPS will not be held liable for either texting or internet usage charges that occur from the use of an PCD. It is the user's responsibility to know the usage options that are available to them, such as the number of texts available, or whether or not their service plan includes Internet.

● CPS will not be held liable for the content already existing on a user owned devices; this would include music/lyrics, movies, pictures, games, etc.

●CPS will not be held liable for any lost, stolen, or damaged PCDs. Users are encouraged to take their

PCDs home every day after school.

● The user bringing personal technology to school agrees to be responsible for and to reimburse CPS for any damage that they may cause arising out of and relating to the use of the CPS wireless network with his/her personally owned device.

6.0 - GUIDELINES FOR USE OF THE INTERNET

Safety - Children's Internet Protection Act (CIPA)

A. All users will access the internet through an appropriate filter that blocks objectionable (inappropriate and harmful) material. Objectionable material is defined as any visual depiction of obscenity, pornography, or other depictions not appropriate for the viewing audience. The filter is set to automatically block these kinds of web pages. Sites and/or apps that advocate antisocial behavior will also be blocked to the extent possible. An appeal process is provided for users who believe specific sites and/or apps are inappropriately filtered or not filtered. The appeal process is outlined below. Users have the option of using the filter or requesting unfiltered access for greater research flexibility. Users will not access pornographic material regardless of whether or not the filter is used.

B. The safety and security of users is of utmost importance. It is expected that users will never give personal information to a stranger by way of email, chat rooms, social media outlets, or other forms of electronic communications. Electronic mail accounts will be given to users only after signing the Acceptable Use Guidelines form indicating they have read, understand, and are willing to abide by these provisions. Chat rooms and message boards will be blocked to the extent possible through the district's filtering hardware and software. Users may request appropriate chat areas to be unblocked for educational purposes a minimum of one week before students are to use this resource.

C. Unauthorized access to the CPS network is strictly prohibited. Any use of the network for hacking or unlawful activities is strictly prohibited.

D. Disclosure, use, and dissemination of personal identification information regarding minors is strictly prohibited by any user without prior permission by the District Administration.

E. Any attempt to circumvent the District content filter is strictly prohibited.

Content

A. Ultimate responsibility for a school website's content lies with assigned designee. He or she will be identified on the homepage of the website with the title of "Webmaster" or "Web Advisor" and an email link will be provided for comments, questions, or feedback.

B. A "Media Release Form" will be distributed upon a student's initial entry to CPS. Parents or guardians will have the opportunity to prohibit the publishing of a student's name and photograph to the extent which the District has control. If student information is used on a website, ONLY the name, grade level and photograph may be published. (No addresses, phone numbers or other personal information may be published.)

C. The web developer and/or a user may determine that a link to an external website or web page may be beneficial for curriculum purposes or other appropriate situation. Any CPS website containing a link or links to external pages or sites will include this disclaimer on the site's home page: "A link to an external

site does not in any way constitute a district endorsement of its content."

Appeals

A. In case of a disagreement regarding web content between the assigned designee and the party requesting a posting, the assigned designee may elect to appoint a review panel of three staff members to provide advice on the following topics:

i. Relevancy and appropriateness of posting content

ii. Size/space requirements of the proposed material

iii. Other issues regarding a proposed posting

B. After consultation with the review committee, the building principal will have the responsibility of making the final decision concerning the web content for his or her building.

C. If a user believes a website and/or app to be inappropriately filtered he or she should use the web form found on the blocked page to request a review of the site. If the Principal concurs with the user that a website is clearly appropriate for students, then a change will be made in the filter to allow or disallow viewing of the site.

D. If a user believes that a website and/or app that is currently not filtered needs to be blocked, he or she should submit a help desk ticket requesting that it be blocked. If it is clearly evident that the site is inappropriate for the audience, it will be immediately blocked. If it is not readily apparent whether the site is inappropriate, it will be forwarded to the Principal for review.

Web Page Development

A. All CPS district and building websites will be hosted on the CPS's web server and will be part of the CPS's internet domain.

B. Third-party hosted solutions for other CPS related sites (e.g., athletics, clubs, bios, etc.) will be reviewed on a case-by-case basis by the Principal or Superintendent. When reasonable, these sites will be hosted on CPS's web server; however, the District reserves the right to make exceptions when deemed appropriate.

C. A school or staff website may be developed and maintained by a CPS's staff member (principal, teacher, paraprofessional, media specialist, etc.) or a volunteer (student, parent, or community member). If the webmaster is a volunteer, the principal or a designee will be assigned to serve as a contact person between the school and the volunteer. CPS's Guidelines for Technology must be observed.

D. The webmaster will develop and build the website privately, whether in a "test" folder on the CPS's server or on another site with a private URL. After approval is received from the building principal or designee, the site may be uploaded to the district server at the district designated URL.

E. CPS may elect to use social media sites (e.g., Twitter, Facebook, YouTube, etc.) for increased web presence and a way of communicating with the community. Anyone maintaining a CPS social media site is responsible for adhering to the rights and responsibilities defined within this document for Social Media.

F. All CPS websites run in-house or hosted on third-party servers must be monitored for appropriate content and updated regularly. Each webmaster is responsible for approving all content, removing any inappropriate content, and ensuring compliance with any student media release forms.

7.0 - GUIDELINES FOR USE OF SOCIAL MEDIA

RIGHTS:

● Each user has the conditional right to access the District provided social media environment (e.g., Google+) to facilitate personal growth in technology and collaboration. While staff are allowed access to public social media outlets (e.g., Facebook, Twitter, Linked In, lnstagram, etc.) for school related activities, students will NOT be granted access to these sites from District-owned computers without prior approval from a teacher or building administrator as there is no way to filter the content available on these sites.

● While CPS recognizes it cannot guarantee a sterile environment for students, it will take necessary steps to ensure the safety of our students and staff.

● Also, the District reserves the right to establish online accounts for students under the age of 13 for educational use with proper parental consent to be in compliance with Federal COPPA regulations.

RESPONSIBILITIES:

● The user is responsible for using social media outlets in a respectful, professional manner.

● The user is responsible for keeping any personal accounts completely separate from any school related accounts.

● Staff are NOT to initiate or accept any requests from students to join a social network being used for personal purposes.

● Staff are NOT to post any pictures of students on any social media sites for personal use.

● The user is responsible for adhering to the media release request of each student prior to posting any photos of students on any social media website for educational use.

● Staff are NOT to interact with students in any inappropriate manner outside of acceptable academic interactions and uses.

8.0 - GUIDELINES FOR USE OF CLOUD STORAGE AND/OR SERVICES

RIGHTS:

● Each user has the conditional right to use cloud storage and/or services (e.g., iCloud, Dropbox, Google Drive, Skydrive, Educreations, NearPod, etc.) for storing and maintaining school related instructional files as long as these files do NOT contain any student or staff identifiable information without first properly securing the data in an encrypted manner, ensuring your browser has https encryption. The District encourages the use of these sites and services as a way to improve efficiencies and reduce storage and backup costs for the District.

● Desktop installations of software to interface with such sites and services will be reviewed on a case-by--case basis by the CPS Information Services Team.

● Each user must also understand that CPS CANNOT guarantee the availability of such third-party services. Any files needed for a specific task should be brought down to the local machine as a backup

and should be deleted when no longer needed.

● Also, the District reserves the right to establish on line accounts for students under the age of 13 for educational use with proper parental consent.

RESPONSIBILITIES:

● Each user is responsible for selecting the tool that works best for them.

● Each user assumes a personal responsibility when using third-party sites and/or services. Online resources and direct communication with the vendor shall be used by the individual to troubleshoot any issues related to these sites and/or services. CPS may attempt to assist with resolving any issues within reason but CANNOT be expected to be an expert on every product available.

● Each user must fill out the Personally Identifiable Information (PII) Submission Form for any service that houses student data.

● Each user must verify that the site has met the SOC1 / SOC2 level of security standards. Supply a copy of the report to the technology office.

● Each user is responsible for NOT storing staff and/or student sensitive information in the cloud.

● Each user is responsible for ensuring both FERPA and HIPPA compliance.

● Each user must provide any school related documents stored in the cloud that are part of a FOIA request.

● Each user must keep personal accounts separate from school related accounts.

9.0 - DISCIPLINARY ACTION FOR VIOLATION OF THIS POLICY

The guidelines on the preceding pages are not all-inclusive, but only representative and illustrative. A user who commits an act of misconduct that is not listed may also be subject to disciplinary action.

Staff are responsible for abiding by all the policies and procedures set forth in this document. Failure to do so may result in disciplinary action up to and including termination and/or legal action.

ACCEPTANCE OF THE STAFF ACCEPTABLE USE POLICY

Please complete the following information:

Staff Member's Full Name (please print): _____

I have read and agree to abide by the Staff Acceptable Use Agreement. I understand that any violation of the terms and conditions set forth in the Agreement is inappropriate and may constitute a criminal offense and/or result in discipline up to and including discharge. As a user of the District's computers/network and the Internet, I agree to communicate over the Internet and the Network in an appropriate manner, honoring all relevant laws, restrictions, policies and guidelines.

Staff Member's Signature: _____ Date: _____

cc: Personnel File

The Superintendent is responsible for determining what unauthorized or inappropriate use is. The Superintendent may deny, revoke, or suspend access to the Network/Internet to individuals who violate the District Staff Acceptable Use Agreement, and take such other disciplinary action as is appropriate pursuant to the applicable collective bargaining agreement and/or Board Policy.

Please complete and return this form to the Business office.