ACCEPTABLE USE POLICY (AUP)
for Contracted Employees

Internet access has been available in the Charlton County School System since 1997. We are very pleased to continue to provide access to our schools. Our goal in providing this service is to promote educational excellence in the curriculum by facilitating communications for resource sharing and innovation.

Therefore, it is the belief of the Charlton County School District that the use of telecommunications, including the Internet, in instructional programs is an educational strategy, which facilitates communication, innovation, resource sharing, and access to information. Use of the Internet must be in support of education and research and consistent with the educational mission, goals, and objectives of the school system.

Charlton County School System (CCSS) will enforce the administrative procedures included in this policy. This policy does not purport to be an all-inclusive list of inappropriate behaviors. Failure to comply with these administrative procedures shall be grounds for revocation of privileges, potential disciplinary and/or appropriate legal action.

ELECTRONIC USE GUIDELINES

The Charlton County School System (CCSS) guidelines provide for contracted employees to become aware of their responsibilities.

If a CCSS user violates any of the following provisions, his or her access may be terminated. Disciplinary actions may be taken that could result in the initiation of legal action.

Employee Due Process:

The site administrator or designee will investigate allegations of all employee violations of the *CCSS Internet Acceptable Use Policy/Procedures*. The contracted employee will be notified and provided an opportunity to respond to the allegations. Activities involving the school system's computers or on the Internet that are in violation of the CCSS *Acceptable Use Policy/Procedures* will be handled in accordance with those documents, and appropriate legal authorities will be contacted if there is suspicion of illegal activity.

Student Due Process:

If a Charlton County School System student violates any of the following provisions, his or her access may be terminated. Disciplinary action may be taken which could result in suspension or initiation of appropriate legal action.

The site administrator or designee will investigate allegations of student violations of the *CCSS Internet Acceptable Use Policy/Procedures*. The student will be notified and provided an opportunity to respond to the allegations. Activities on the Internet that are in violation of the *Charlton County School System Code of Conduct* will be handled in accordance with that code. The student's parent(s) and appropriate legal authorities will be contacted if there is any suspicion of illegal activity.

TERMS AND CONDITIONS

I. ACCEPTABLE USE

Access to the school's Electronic Network (EN), which refers to the use of the Internet/On-line/Email/School Web Page programs are provided for educational purposes and research consistent with the school system's mission and goals.

II. PRIVILEGES

The use of the school system's **EN** is a privilege, not a right. Inappropriate use may result in the cancellation of those privileges. The Superintendent or designee(s) shall make all decisions regarding whether or not a use has violated these procedures and may deny, revoke, or suspend access at any time.

III. ACCEPTABLE AND UNACCEPTABLE USE GUIDELINES FOR ALL USERS

The **USER**, refers to all students, staff employees, contracted employees, are responsible for all his/her actions and activities involving the network/internet/emailing.

Guidelines:
USER activities are <u>permitted</u> and <u>encouraged</u>:

1. School work;
2. Original creation and presentations of academic work;
3. Research on topics being studied in school;

4. Research for opportunities outside of school related to community service, employment or further education.

USERS activities that are <u>NOT permitted</u> when using district or personal technologies include but are not limited to:

A. USERS will NOT access or send materials or communication, which are:

1. Damaging to another's reputation
2. Abusive
3. Obscene
4. Sexually oriented
5. Threatening
6. Contrary to the school's policy on harassment
7. Harassing
8. Illegal

B. USERS will NOT use the network for any illegal activity, including violation of copyright or other contracts or transmitting any material in violation of a school rule or a local, state or federal regulations
C. USERS will NOT copy or download copyrighted material connected to the school system's hardware/software without the owner's permission. Only the owner(s) or individuals specifically authorized by the owner(s) may copy or download copyrighted material to the system. Copying and downloading of any copyrighted material should adhere to Federal Copyright Laws - http://www.copyright.gov/
D. USERS will NOT Plagiarize or represent the work of others as one's own
E. USERS will NOT use the network for private, financial, political, or commercial gain
F. USERS will NOT share their email or network password with anyone
G. USERS will NOT attempt to read, delete, copy, or modify the e-mail of other users and deliberately interfering with the ability of other users to send/receive electronic mail
H. USERS will NOT share online any student or staff personal information
I. USERS will NOT use the email account to conduct commercial or for-profit business activities
J. USERS will NOT view or transmit any racist, sexist, pornographic, obscene, or threatening material
K. USERS will NOT download any materials that are not related to course work
L. USERS will NOT plagiarize or represent work of others as their own
M. USERS will NOT research for inappropriate materials
N. USRS e-mail correspondence will be monitored by the onsite advisor for the online course

O. USERS will NOT upload viruses or other destructive computer files; hack into the district or external computers; intentionally bypassing the district filters; and purposely damaging any data on the network
P. USERS will NOT use of USB, bootable CDs, or other devices to alter the function of computer or a network
Q. USERS will NOT use or participate in the use of online non-educational uses such as games, role-playing multi-user environment, gambling, junk mail, chain mail, jokes, chat rooms, instant messaging
R. USERS will NOT damage or modify any computers, printers, other equipment or network devises attached to the network
S. USERS will NOT use personal email accounts, not district-provided e-mail accounts, on the district network, unless given prior permission by their school level administrator
T. USERS will NOT utilize any software having the purpose of damaging the school system's servers or other user's equipment
U. USERS will NOT posting material unauthorized or created by another user without his/her consent
V. USERS will NOT post anonymous messages in e-mails or on their school webpage
W. USERS WILL send to their building level administrators all message postings or e-mails for prior approval for **ALL** school or non-school community functions
X. USERS will NOT use the network while access privileges are suspended or revoked

IV. WARRANTIES

Charlton County School System makes no warranties of any kind, whether expressed or implied, for the service it is providing. The Charlton County School System will not be responsible for any damages you may suffer. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by network failure or your own errors or omissions.

V. ADOPTED BOARD POLICY FOR PROTECTION OF CHILDREN'S INTERNET SAFETY (Adopted May 21, 2002, Updated June 19, 2012)

It shall be the policy of the Charlton County Board of Education that the school district shall have in continuous operation, with the respect to any computers belonging to the school having access to the Internet:

1. A qualifying "technology protection measure," as that term is defined in Section 1703(b)(1) of the Children's Internet Protection Act of 2000; and

2. Procedures or guidelines developed by the superintendent, administrators and/or other appropriate personnel which provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers

to visual depictions that are (i) obscene, (ii) child pornography, or (iii) harmful to minors, as those terms are defined in Section 1703(b)(1) and (2) of the Children's Internet Protection Act of 2000. Such procedures or guidelines shall be designed to:

a. Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the World Wide Web;

b. Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

c. Provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness, and response in accordance with FCC's Report and Order FCC 11-125 rulings released August 11, 2011;

d. Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;

e. Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and

f. Restrict minors' access to materials "harmful to minors," as that term is defined in Section 1703(b)(2) of the Children's Internet Protection Act of 2000.

CIPA BACKGROUND

Full text of the Children's Internet Protection Act
http://www.fcc.gov/ccb/universal_service/chipact.doc

FCC regulations implementing CIPA; FCC 01-120
http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01120.doc

SLD's FAQ on E-rate certification procedures and timing
http://www.sl.universalservice.org/reference/CIPAfaq.asp

Staff members should become familiar with this procedure. When in the course of their duties all staff members and contracted employees become aware of student violation of acceptable use (Internet) policy, they should correct the student and address the matter in accordance with this procedure and the Board of Education's general disciplinary policies and procedures.

VI. STAFF SUPERVISION/MONITORING

All members of the CCSS staff and contracted employees shall be the responsibility to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Coordinator or designated tech/media person.

In addition:

1. Teachers and administrators are to model and enforce proper computer and technology use. The use of proper copyright restrictions is to be fully enforced.

2. Students are not to use computers for entertainment or time killers. Time spent on computers should be for instruction and curriculum specific use only.

3. Students are not to go to the media center to use a computer unless the teacher has written specific directions for the use of the computer for an assignment. The Media Specialist will approve the request by the teacher and supervise the use by the student. The teacher must be with his/her class in the media center, and the teacher is responsible for monitoring his/her students. Student access may be limited in the media center as decided by the Media Specialist if the teacher does not accompany them.

4. Students and teachers are not allowed to download or install computer disks (data disks or software programs, etc.) into any school computer unless the disk or USB travel drive has been checked on a stand-alone workstation (not connected to the LAN) by virus and security software. Loading any disk or USB travel drive into a computer should be done for evaluation purposes and supervised by the local technology team, media specialist, or technology coordinator.

5. Teachers, students, and administrators are not allowed to load software on computers without the permission of the local school administrator, media staff, and district Technology Coordinator. Loading of software on computers without permission is unacceptable.

6. Copyright restrictions are to be followed and enforced. Each employee and contracted employee is responsible for knowing the current copyright restrictions.

7. The local Media Specialist is to make available copyright rules to teachers and administrators. The Media Specialist should supply proper citation information and procedures for teachers and administrators.

8. Monitoring of computers in all situations is essential. Monitoring practices include walking around labs and helping students during the entire class period, being visible to students the entire time, and checking for improper use. Poor monitoring practices could result in security, hardware, and software damage.

Poor monitoring practices include inability to see computer screens at which students are working, not walking around labs, sitting, and being preoccupied with other work while students are at workstations.

9. Measures necessary to secure teacher work stations include: locking desktop, keeping students away from teacher workstation, providing room arrangements which block student access to teacher workstation, shutting down the computer when the teacher leaves for the day, keeping the mouse and keyboard in a secure place when the teacher is expecting a sub, locking the room when the teacher leaves at any time, and advising students as to the penalties for improper computer use.

VII. INTERNET FILTERING

The Charlton County School System is presently using an advanced filtering solution to choose access and manage the type and level of online information that is most appropriate and relevant to the system's educational needs and goals, as well as reduce legal liability. The filtering software in place uses a sophisticated research process involving human review to continuously comb, analyze, and catalog each Internet site. This provides the most powerful, flexible tool available for assisting in the enforcement of the acceptable use policies (AUP) for the Charlton County School System.

It is prohibited to use personally owned equipment such as, but not limited to, smart cards, wireless cards, etc, to bypass the filtered Internet that CCSS has put in place.

Software and websites that are used to bypass the filter such as anonymizers and proxies are prohibited.

VIII. PASSWORDS

Access to the network and PC systems is limited to authorized users. Each user is assigned a login name and password. Student accounts are provided at each school without a password but restricted access to network accounts. All staff employee passwords are set for the network and programs by the administrative staff. The only password users may personalize is their e-mail account.

For all e-mail accounts users they will be prompted to change their password on the first time logging on his/her e-mail account.

Suggested passwords guidelines to adhere:

Require to be at least six (6) characters in length
Require being alphanumeric
Require they contain at least one capital letter
Require they be changed annually

Examples: HaPpY8 (Passwords are case sensitive)
wOndeRfuL8

Users should not display their passwords anywhere out in the open, or near the computer such as under the keyboard or on the monitor. Each user is given three tries to successfully log on to the network or online programs or their email account. **If the user after the third try does not log on, the user account will be locked.** The user will need to contact the Technology Coordinator by phone or email to get his/her account unlocked and get his/her password reset if necessary.

IX. COMPUTERS

Users will log off or shutdown his/her computers at the end of the week. Users will lock the computer when they take a break or if the computer is left unattended for any extended period. A domain policy will be implemented that will automatically lock workstations when no activity has been detected after 30 minutes. Computer(s) will be secured if a staff member is not there to monitor them.

At no time will personal equipment (computers, laptops) or peripheral equipment (PDA's, digital cameras, external drives, etc) be used on the network only by prior written approval from the administrator and media staff at each school. This is to ensure that malicious software and viruses do not breach security.

X. SOFTWARE

To ensure the integrity of the network and programs running on the network, users are expressly prohibited from installing or running unapproved software programs. If users receive written approval from the administrator and designated tech person, they may load and use software. They may load other software by prior written approval. The school system complies with copyright and license laws by only installing and running software for which the school system is an authorized user and has obtained a license agreement.

All software installations must be coordinated through the tech office and media staff in order to ensure compatibility with the server and workstation operating systems that are used throughout the school system.

Copyrighted material must not be placed on any system connected to the network. No software should be uploaded to the servers.

If prior approval is not acquired before using personal equipment and/or software on the CCSS network, the equipment and/or software may be confiscated. If a user needs written approval for use of personal equipment and/or software, they must contact the media staff or administrator at your school.

XI. VIRUS PROTECTION

All software must be run through an anti-virus package before being installed on the network. All computers in the school system will have anti-virus and anti-spyware software loaded on them. All files downloaded from the Internet must immediately be scanned for viruses. These programs are all supervised by the media specialist and technology coordinator.

XII. SECURITY

Network security is a high priority:

1. If the user identifies or perceives a security problem or a breach of these responsibilities on the EN, he/she should immediately notify the administrator or media staff – the problem should not be demonstrated to others.

2. Attempts to login to the network as a system or site administrator will result in immediate cancellation of user privileges.

3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

4. Any CCSS user who gives another user their login information will have their network and computer privileges revoked.

XIII. NETWORK ETIQUETTE

The user is expected to abide by the generally accepted rules of the network etiquette. These include but are not limited by the following:

A. Be polite. Do not become abusive in messages to others.
B. Use appropriate language. Do not swear, or use vulgarities, or any other inappropriate language.
C. Do not reveal the personal addresses or telephone numbers of students.
D. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to **ALL** mail. Messages relating to or in support of illegal activities may be reported to the authorities.
E. Do not use the network in any way that would disrupt its use by other users.

IXX. **EMPLOYEES ELECTRONIC COMMUNICATION GUIDELINES (E-MAIL)**

Contracted employees are not provided with an email account. Source4Teachers supply the email accounts.

E-mail messages created using CCSS e-mail system are property of CCSS and are not to be considered private. CCSS reserves the right to monitor inspect, copy, review and store at any time all e-mails. In addition, CCSS has the right to disclose e-mails, attachments, and images to the courts, law enforcement, and other third parties without the contracted employee's consent.

Contracted employees should assume that anyone could read what is sent and received. Account holders shall be held accountable for everything stated and therefore should not post anything that he/she does not want to see revealed to the public.

Disclosure or sale of any e-mail addresses to outside entities is prohibited.

The CCSS e-mail system is designed to provide electronic communication and use of related resources. CCSS users with e-mail access shall adhere to the following procedures:

All electronic communication created, sent, or received via the CCSS e-mail system is the property of the CCSS school system. CCSS users shall not have any expectation of privacy regarding this information. CCSS 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, CCSS reserves the right to disclose text or images to law enforcement agencies without the user's consent.

The superintendent or his/her designee is permitted to access another user's e-mail without consent.

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

The CCSS e-mail system shall not be used by contracted employees to solicit for non–school system business.

The user shall delete inappropriate messages and/or programs.

Administration and/or CCSS Human Resources shall report all changes in worker duties or employment status to the Principal or Technology Coordinator or Media Specialist. Such changes include termination of employment, lateral moves or any

job change that would require an update of network/e-mail account information or a change in network/e-mail access.

When an employee leaves, the Administrator and/or Human Resources person shall notify the Technology Coordinator immediately. The contracted employee's e-mail account shall be placed on hold for a period of 30 days unless notified by the superintendent or designee to hold the account for an extended period. If this notification is not given all e-mails, folders, and attachments may be deleted at the expiration of this period. The contracted employee's manager/supervisor can request access to the former contracted employee's e-mail during this period to review messages for required retention.

Access to e-mail accounts under investigation shall be restricted without notice until authorized by the Superintendent or designee.

While CCSS 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 come across 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. CCSS is not responsible for the views expressed by individual users via web pages, electronic mail or other on-line communications.

XX. FILE & ELECTRONIC DOCUMENT MANAGEMENT

Retention of documents on non-administration shares **will be purged** between the periods of **July 1 through July 15** of each year. It will be all staff members' responsibilities to archive these items digitally.

Electronic Documents

Sending email attachment size	20 MB (limited by Gmail)
Receiving email/attachment size	20 MB (limited by Gmail)
Account holding mailbox size	Unlimited (Gmail)
Folder holding incoming email	By user filter settings
Deleted items & SPAM folder	30 days purge cycle
Calendar appointments	By user filter settings (Gmail)
Documents on File Servers/Teradrives	Purged when employment ends

XXI. VANDALISM

Vandalism will result in immediate cancellation of privileges and possible disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy. The use of CCSS computer equipment should not be used for unauthorized access to other networks.

XXII. **USER INFORMATION**

All CCSS users must complete and return a new AUP Agreement form and Web Page form annually. (Contracted employee – AUP Agreement/Webpage Agreement forms and Student/Parent – AUP Agreement Form)

XXIII. **ACCEPTANCE**

All terms and conditions as stated in this document are applicable to the Charlton County School System. These terms and conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understanding of the parties. These terms and conditions shall apply to federal and state legal regulations.

IFBG-R

CONTRACTED EMPLOYEE ACCEPTABLE USE AGREEMENT (CEN)

Each contracted employee will be required to read and understand all Charlton County Board of Education policies governing user access and use of the WAN/LAN Networks, Internet, and School Teacher Web Pages.

I have read, understand, and will abide by the ***Charlton County School System Acceptable Use Policy for the Electronic Network & Internet*.** I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school system disciplinary action and/or appropriate legal action may be taken, up to and including employment termination.

I further agree to promote the enforcement of the regulations in supervising student Network & Internet use.

_____

Contracted employee's Name (please print)

_____ _____/_____/_____

Contracted employee's Signature Date

Personal Computing Equipment
On the Charlton County Schools Network

No personal computing equipment shall be placed on the CCSS network prior to meeting the following conditions and signing of this form. Use of this equipment on the CCSS network requires compliance with current district Internet Acceptable Use Policies.

1. The building administrators designated school tech person (STP) will check the hardware; OS patch, Virus definitions, and network compatibility with our network prior to connecting the device to the network.
2. All updates and patches for the Operating System must be up to date.
3. Virus protection must be installed with virus definitions kept up to date.
4. All software must be licensed by the contracted employee; CCSS will not provide or load software onto a personal computing device.
5. All hardware and software issues, other than the connection to the CCSS network, will be the responsibility of the contracted employee / owner of the device. CCSS will not provide technical support for personal hardware other than the connection to the CCSS network.
6. The STP may deny any device that does not meet all of the above criteria. In such a case, the STP will inform the contracted employee of the specific deficits of the device so that they can either remedy the deficits or choose not to connect the device to the network. This also applies to any device to be found with deficits listed above, viruses, or faulty hardware. The STP will disconnect any equipment that becomes a liability to the safety and security of the CCSS network even if previously approved to not be a liability.
7. Any theft, damage or vandalism that occurs to the device will be the responsibility of the contracted employee / owner of the device in question. Personal devices will not be covered under the CCSS insurance policy. The contracted employee will assume this risk and does not hold CCSS liable for any damage that occurs to a personal network device.

Equipment used to connect to or modify current CCSS network infrastructure is not authorized for use. This equipment would include, but is not limited to; network hubs, switches, wireless access points, routers, VOIP phone devices; personal wireless phone connectivity through the CCSS network.

I have read and understand the above guidelines relating to any personal computing equipment that I bring into CCSS. I agree to the terms and conditions stated above.

Name: _____

School: _____

Room # _____

Equipment Description brought in:

_____

_____

Signature: _____ Date: _____