SOUTH CAROLINA GOVERNOR'S SCHOOL
for Science & Mathematics

APPROPRIATE USE POLICY

The Appropriate Use Policy (AUP) pertains to all users of GSSM networks, contracted services, and any and all other technologies provided by or on behalf of the school. The term *user* includes, but is not limited to, employees, students, alumni, visitors, contractors, program applicants, job applicants, program participants, and volunteers.

GSSM's computer network supports school operations, communications, research, and education by providing access to useful shared resources and facilitating collaborative work. Uses that support these purposes and facilitate school operations receive the highest priority. Other uses that interfere with GSSM objectives are prohibited.

By definition, a network is a shared resource. GSSM's network is shared by its students, teachers, and administration. Those who use the network accept the responsibility to use it appropriately. This Appropriate Use Policy describes those responsibilities and the rules that apply to users of the GSSM computer network.

A. Ethical and Behavioral Standards

Those who use the GSSM network are expected to follow the same standards of conduct and communication that would be expected in face-to-face encounters. Some responsibilities are unique to the environment created by computer networks and are addressed here:

1. **Online Safety**
   GSSM cares about the safety of the community and is deeply concerned about the increasing incidents of assault by those who locate or arrange meetings with their victims through Internet-based social networking services. These services can be dangerous when personal information, particularly information that can lead to the identification or location of a person, is published openly. GSSM strongly encourages everyone to secure their profiles so that they are not visible to strangers.

2. **Online Harassment**
   GSSM's policies against harassment are in effect whenever and however community members encounter each other, including online encounters. The use of Internet services within and beyond the control of the school to harass or defame another person is a violation of GSSM rules and will be vigorously investigated and prosecuted. When harassment involving non-GSSM services is observed or reported, the school may engage law enforcement agencies and the courts to compel the service provider to disclose identifying information about the harassing party.

3. **Protected Information**
   Education records, health information, confidential information, information which may be of a personal or private nature must be transmitted and stored in an approved encrypted format. Such information may only be accessed using authorized equipment maintained and authorized by GSSM and by authorized GSSM personnel. For more information, refer to the GSSM Information Security Policy.

4. **Online Identity/Login Credentials**
   GSSM provides network users with credentials (username and password) for the purposes of accessing network resources. These credentials are intended to be used only by the person to whom they are assigned. Credentials assigned by GSSM must be kept secret and may not be divulged to anyone else. The person to whom network credentials are assigned is responsible for all activities that occur when those credentials are used. Further, it is a violation of GSSM rules for a person to impersonate someone else by either using their credentials, or any other means that might obfuscate

identity. GSSM students and employees may be provided credentials to access online databases while using the Coker University library. While these credentials are issued by Coker University, their use is governed by this AUP. Unless otherwise authorized in writing, login credentials expire upon separation from the school (graduation, dismissal, withdrawal, or other termination).

5. **Intellectual Property**
   As an educational institution that values the contribution of research to the quality of life and civilization, GSSM strongly supports the rights of owners of intellectual property. Many Internet services facilitate sharing and collection of digital content like music and movies in violation of the rights of their owners. Acquiring, possessing, or sharing digital content in violation of copyright is illegal and prohibited at GSSM.

6. **Prohibited Access**
   Attempting to access protected information without authorization is a serious violation of GSSM rules, in addition to applicable governing laws. Users are prohibited from all activities that could inappropriately reveal the existence or configuration of servers, databases, network services, or security features. Scanning to discover network resources is expressly prohibited.

6. **Pornographic & Other Objectionable Material**
   All persons who use the GSSM network are prohibited from viewing, accessing, sending, or possessing pornographic material on GSSM-owned computers, via the GSSM network, while on the GSSM network, or at a GSSM-sponsored event. Attempts to circumvent, disable, or otherwise render content filter measures ineffective are a violation of GSSM rules. It is important to note that when students use networks off campus, the school is unable to regulate the content available to them. Particularly during summer research internships and while conducting assignment research at the Coker University library or any other collegiate library, GSSM students will access networks not equipped to prevent access to pornographic material. Colleges and universities are only required to enforce their own published access standards, which will vary between institutions.

7. **Conservation of Shared Resources**
   Network resources may be overwhelmed when used indiscriminately. Therefore, it is the responsibility of each person who uses the GSSM network to conserve resources where possible so that they are always available for others to share:

   a. Internet circuit capacity
      GSSM utilizes a commercial-grade connection circuit to provide Internet access to the campus. Priority for using this service is given to educational and campus operation purposes. GSSM will manage this resource by prioritizing Internet traffic, limiting or eliminating interfering services, and other means as necessary.
   b. Message and file storage
      GSSM servers provide spaces to store messages and files. They are intended to support educational and campus operations. Therefore, they should not be used to store media collections or for other recreational purposes. GSSM servers may never be used to store illegal content.

B. Using Your Computer at GSSM

GSSM encourages students to bring computers to school for use in their rooms, classrooms (when allowed by their teacher), and around campus. Employees sometimes use the school's WiFi system with their personally owned phones and tablets. Attaching a personally-owned device to the GSSM network indicates acceptance of this AUP and places specific responsibilities upon the owner:

1. **Owner Responsibilities**
   Computer owners are responsible for ensuring that their computers are virus-free prior to connecting to the network. Computer owners may be held responsible for damage created by computer viruses, or other activity originating from their computer. When it is determined that a computer is threatening

the stability of the network or other computers, it will be removed from the network immediately. Owners are also responsible for maintaining their own computers. GSSM does not have staff available for computer repair. Computers should be in good working condition when they arrive on campus. Owners should back up their important files often to prevent loss in the event of a computer failure.

2. **Antivirus Software is Required**
   Every computer that is connected to the GSSM computer network must have effective, up-to-date antivirus software installed at all times. This protects the computer owner as well as others on the network. Computers found to have out-of-date or no antivirus software installed maybe removed from the network.

3. **Dynamic Network Addressing**
   The GSSM computer network automatically assigns IP addresses to each connected computer. This address must not be tampered with or changed. While assigned IP addresses are dynamic and subject to change without warning, in practice these numbers will rarely change throughout the school year.

4. **Network Registration**
   Computers and other devices are registered to their owners when they log into WiFi and present a username and password, or when they attached to a network port in a are student's room. Attempting to conceal the ownership of a computer is a violation of school rules.

5. **Accessible Hours in Residence Halls**
   The computer network in the residence halls is available Monday through Thursday from 5:30am until 1:15am, and from 5:30 am Friday through 1:15am on Monday of each week. These hours may be modified in the event of an academic Saturday.

6. **Protected Information**
   It is a violation of state regulations for protected information to be copied to or stored on personally owned devices. Protected information includes education records, health information, or any other information that is considered to be GSSM Confidential or a personal and private nature to an employee or student.

7. **Prohibited Devices**
   Certain network devices can interfere with network operation. Any kind of DSL/Cable router has this potential and is prohibited on the network. WiFi access points, hot stops, routers, and other devices that provide WiFi network services to others reduce the number of channels available to the GSSM network, reducing performance in the area where they operate. Only wireless devices acting as clients of the school's WiFi network are allowed.

8. **Prohibited Software**
   Software that creates durable connections to Internet services, or that allow others on the Internet to access, share, or control computers on the GSSM network represent security risks and are therefore prohibited. Any software that scans networks or computers for vulnerabilities, any software that interferes with the GSSM network or devices attached to it, or any software that facilitates circumvention of any GSSM rule is prohibited.

9. **Wireless Network**
   Govienet is GSSM's wireless network for students. The password for connecting to Govienet is distributed regularly. Once connected to Govienet, an additional username and password is required to gain access to the Internet. These credentials are requested infrequently. Using another student's credentials is prohibited as is using other wireless networks not intended for student use. A guest network is available for visitor use and for devices owned by employees. Instructions for connecting

to it are posted in the main lobby. Only authorized employees using school-owned laptops and similar wireless devices may connect to the administrative WiFi network.

10. **Microsoft Office**
    As part of its site licensing agreement with Microsoft, students and employees may download MS Office to their computers and portable devices. Each person may install the software on up to five personally owned devices which may include phones and tablets. The installation screen is accessed through the Outlook portal (https://outlook.office.com). GSSM provides this service as a convenience and makes no guarantees regarding compatibility, fitness, or availability for any particular task. Anyone who downloads and installs Microsoft products accept any and all license terms applicable to their use. Access to Outlook, Onedrive, and any associated installations of Microsoft Office will stop working when students or employees leave the school, although documents created with the software will still be functional.

11. **Compatibility**
    GSSM makes no guarantee of compatibility between personally-owned equipment and its networking equipment, services, software, etc.

C. Privacy

In order to protect the computer-using community and to enforce GSSM rules and policies, the school reserves the right to examine, restrict, or remove any material that is on or passes through its network. Such activities are not undertaken routinely or lightly. In addition, specific information about computer use is collected and preserved over time:

1. **Internet locations visited**
   This information is logged for each Internet user and device.

2. **IP addresses assigned to each computer**
   When an IP address is assigned, the hardware address of the computer, the IP address assigned, the date and time of the assignment and location of the computer requesting the address are recorded.

3. **Log in/out information**
   User name, network location, date and time are recorded when logging into or out of some network resources.

There are privacy issues associated with using public GSSM web sites that are described at: http://www.scgssm.org/privacy-policy.

D. AUP Violations

Violations of the AUP may result in temporary or permanent loss of network use privileges. Depending on the nature of the violation, additional disciplinary actions may be taken.

E. Amendments

These policies may change from time to time as circumstances warrant. The most current version will always be posted online at http://www.scgssm.org/aup..

Updated May 8, 2019