HORRY-GEORGETOWN TECHNICAL COLLEGE

PROCEDURE

Number:	7.2.3.1
Related Policy:	7.2.3
Title: Acceptable	Use Policy for Network Services and the Internet
Responsibility:	Vice President of Information Technology
Original Approval Date:	06-01-2000
Last Cabinet Review:	01-04-2017
Last Revision:	01-04-2017

_____

President

I. Public Record

All users of the College's Information Technology (IT) resources accept that all electronic communications, regardless of their subject, content, nature or format, are "public records" of the State, subject to release through the South Carolina Freedom of Information Act. Except for the limited exemptions specified in Section 30-4-40 of the Act, neither the institution, nor the individual has a right to privacy. Therefore, all electronic actions and communications should be created and distributed under the assumption that the whole world may see them.

II. General Principles

1. Use of network services provided by the College may be subject to monitoring for security and/or network management reasons. Users of these services are therefore advised of this potential monitoring and agree to this practice.

2. Users may be subject to limitation on the use of the networks as determined by the appropriate supervising authority.

3. Users who violate any copyright declarations are acting outside the course and scope of their employment or other authority and the College is relieved of any legal responsibility thereof. Users will be personally responsible and liable for such infringing activities.

4. By participating in the use of IT resources provided by the College users agree to be subject to and abide by this policy for their use. Willful violation of the principles and provisions of this policy may result in disciplinary action.

5. This document may be updated on an as-needed basis and is subject to annual review.

III. Specific Provisions

Users shall:

1. Use the network only for official business and for education and research purposes, and access those files and data that are their own, that are publicly available, or to which they have authorized access.

2. Refrain from monopolizing the system, overloading the network with excessive data or wasting computer time, connect time, disk space, printer paper, manuals or other resources.

3. Protect their user ID, password, and system from unauthorized use.

4. Assume responsibility for any charges associated with billable services unless appropriate authorization has been obtained.

Users shall not:

1. Use the network for illegal or unlawful, or immoral purposes or to support or assist such purposes. Examples of this would be the transmission of violent, threatening, defrauding, obscene or otherwise illegal or unlawful materials.

2. Use mail or messaging services to harass, intimidate or otherwise annoy another person.

3. Use the network for private, recreational, non-public purposes including the conduct of personal commercial transactions.

4. Use the network for commercial or partisan political purposes.

5. Use the network or other college equipment for personal gain such as selling access to a user ID or by performing work for profit with college resources in a manner not authorized by the College.

6. Use the network to disrupt network users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising propagation of computer “worms” and viruses, and sustained high volume network traffic which substantially hinders others in their use of the network.

7. Attempt to circumvent or subvert system or network security measures.

8. Intercept network traffic for any purpose unless engaged in authorized network administrative duties.

9. Make or use illegal copies of copyrighted software or other mediums, store such copies on the system, or transmit them over college or state networks.