Appendix B. Peer-to-Peer (P2P) File Sharing

For more information, please review the official policy on the College of Charleston website at http://policy.cofc.edu/

1. PURPOSE OF POLICY

The purpose of this Policy is to detail the College's plans to effectively combat the unauthorized distribution of copyrighted material by Users of the College's Computer Network and Information Technology Resources, without unduly interfering with the legitimate educational and research use of the Network; and to provide for annual disclosures to students on the College's policies and sanctions related to unauthorized peer-to-peer file sharing, as required by the Higher Education Opportunity Act of 2008 (the "HEOA").

Additionally, this Policy is intended to mitigate the College's potential exposure to security risks and liabilities associated with the exploitation of P2P applications to illegally use, distribute and/or store copyrighted materials on the College's Network.

2. POLICY STATEMENT

The College is committed to preventing, in so far as practicable, the misuse of the College's Computer Network and other Information Technology Resources, including but not limited to, the unauthorized distribution of copyrighted material by Users of its Computer Network. It is the College's intent to maintain the integrity of its Computer Network, without unduly interfering with educational and research use, by utilizing the methods described in Section 6.0 of this Policy. This Policy does not ban legal P2P file sharing through use of the College Network, and the College will continue to support technologies that facilitate legitimate information dissemination and academic collaboration.

3. APPLICATION

3.1 Individuals.

This Policy applies to all individuals (students, faculty, staff, College volunteers, contractors, consultants and other members of the public) who use the College's Network and/or Information Technology Resources ("Users").

3.2 Resources.

This Policy also applies to the College's Network and all other College Information Technology Resources; any other information technology resource made available to the College community through a College vendor-sourced network; and other electronic device regardless of ownership when such device is actively using the College Network or is otherwise interfacing with a College Information Technology Resource. The physical location of any computer or other device is irrelevant to whether or not a violation of this Policy exists.

4. DEFINITIONS

4.1 The terms below shall have the meaning ascribed next to each:

(a) **College Computer** - Any computer that is owned, leased or rented by the College of Charleston whether such computer is located on or off College premises.
(b) **College Network** - Any part of the College's data, voice or video network physically located on any College owned, leased, or rented property or located on the property of any third party

with the permission of that party. This includes devices on such network assigned any routable and non-routable IP addresses and applies to the College's wireless network and the network serving the College's student residence halls and houses, and any other vendor supplied network made available to the College community.

(c) **Digital Millennium Copyright Act (DMCA)** - A federal law passed in 1998 that revised copyright law to, among other things, define how alleged copyright infringements are to be handled and to establish liability limitations for "online service providers ."

(d) **DMCA Notice** - DMCA or copyright infringement notices are warnings issued from the copyright holder or a representative of the copyright holder. These copyright holders have identified computers on the College's Network as having potentially violated the DMCA and issue warnings regarding the particular infringement to the College.

(e) **IT**-The College's Division of Information Technology.

(f) **Information Technology Resources** - The College Network and all College computers and computer components, electronic storage devices, wiring, and electronic transmission devices owned, leased, rented or operated by the College or and all College owned or licensed software.

(g) **Peer-to-Peer (P2P)** - A network environment where participants share their resources (such as files, disk storage, or processing power) directly with their peers without having to go through an intermediary network host or server.

(h) **Peer-to-Peer File Sharing Applications** - Programs or services that use P2P technology to share music, movies, software, or other digitally stored files.

5. PROHIBITED ACTIVITY

5.1 Violations.

It is a violation of this Policy to use the College Network or any Information Technology Resource of the College to distribute, download, upload, stream, scan, store or share any material including software, data, document, sound, music, video, picture, design, graphic, game, or any other electronic file when:

(a) the file is copyrighted but distribution to the User has not been authorized by the copyright owner;

(b) the file is copyrighted but distribution to the User has not been authorized by the copyright owner;

(c) when the material is considered by the College to be Protected Information under the College's Privacy Policy and the User is not authorized to access that information or to access that information for the purpose intended; or

(d) when the User's intent is deployment or introduction of any virus or malware on any Information Technology Resource.

5.2 Circumvention Prohibited.

Users of the College's Information Technology Resources shall not attempt to circumvent, bypass, defeat, or disrupt any device, method, or technology implemented by the College for the purpose of

implementing this Policy.

6. PROCEDURES FOR COMBATING UNAUTHORIZED P2P FILE SHARING

6.1 Technology-Based Deterrents

(a) Use of Deterrents. The Senior Vice President for Information Technology (CIO) will utilize technology-based deterrents to combat the unauthorized distribution, downloading, uploading, streaming, scanning, storage or sharing of copyrighted material by Users of the College's Network , and will periodically confer with the President's Executive Team to ensure that all such technology-based deterrents then employed by the College do not unduly interfere with legitimate educational and research uses of the College's Network.

(b) Types of Deterrents. At least one technology-based deterrent must be in use at all times with respect to the College's Network. As determined appropriate from time to time by the CIO, technology-based deterrents may include, but not be limited to, one or more of the following:

- Bandwidth shaping;
- Traffic monitoring;
- Accepting, aggressively pursuing and responding to DMCA notices; and/or
- By using commercial product to reduce or block illegal file sharing.

6.2 Directive Authority.

For the purpose of implementing this Policy, the CIO shall have directive authority over all vendors to the College, including those vendors who supply internet services to student housing, to direct that such vendors use appropriate deterrents to reduce or prevent illegal file sharing and other violations of this Policy. When exercising such directive authority, the CIO shall consult with the appropriate contract administration officer of the College and ensure that all corrective actions are taken in accord with relevant contract documents.

7. EDUCATE AND INFORM THE COLLEGE COMMUNITY

7.1 Mechanisms.

The College shall employ, at a minimum, the mechanisms described in Sections 7.2 and 7.3 for educating and informing the College community about the appropriate and inappropriate uses of copyrighted material.

7.2 Institutional Information for Students.

The College will make readily available to enrolled and prospective students the College's policies and sanctions related to copyright infringement including:

(i) a statement that explicitly informs its students that the unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may subject the student to civil and criminal liabilities;

(ii) a summary of the penalties for violation of Federal copyright laws; and

(iii) this Policy.

The disclosure required by this Section 7.2 shall be made in the following manner:

(a) Enrolled Students - The Office of the Dean of Students shall be responsible for disseminating annually a notice (of the general nature as set forth in Appendix A to this Policy) to enrolled students regarding the institutional information described in this Section. The methods of dissemination of the Notice may include the College web pages, one-toone e-mail, orientation presentations, student publications and publication in the Student Handbook and the my.charleston portal.

(b) Prospective Students - The Division of Enrollment Management will post or link a copy of the institutional information on the Admissions web portal for review by prospective students.

7.3 Educating the Campus Community.

Other members of the Campus community shall be provided institutional information as follows:

(a) The Addlestone Library will post and maintain the College's Copyright Guidelines and this Policy on its webpage.

(b) The Division of Information Technology will publish and maintain a webpage devoted specifically to this Policy and P2P file sharing. Such webpage shall contain a list of FAQs and How-To Guides that instruct the campus community about appropriate and inappropriate uses of P2P applications; a summary of penalties for violation of Federal copyright laws; a summary of the results from the periodic review of the effectiveness of the College's plans to prevent the unauthorized distribution of copyrighted materials by Users of the College's network; and a list of legal alternatives for downloading or otherwise acquiring copyrighted material. The College reserves the right to block the use of any application on the College's Network when it has a reasonable basis to conclude that such application is being used for improper purposes in violation of this Policy.

(c) The Ask the Cougar query on the College's web site shall be modified, as appropriate, to refer to the webpage described in subsection (b) of this Section 7.3 when queries are made relating to the subject matter covered by this Policy.

7.4 Summary of the Penalties for Violation of Federal Copyright Laws.

The CIO and the Dean of Students, in consultation with the Office of Legal Affairs and utilizing the Federal Student Aid Handbook , shall annually publish a summary of the penalties for violation of Federal copyright laws (the "Summary''). Dissemination of the Summary shall be as follows:

(a) The Dean of Students is responsible for including the Summary in the annual Notice to enrolled students;

(b) The Assistant Vice President for Admissions and Financial Aid is responsible for including the Summary in institutional information made readily available to prospective students; and

(c) The CIO is responsible for posting the Summary on the IT web page dedicated specifically for P2P as further described in section 7.3(b).

8. ENFORCEMENT

8.1 Generally

The College's Network, Computers and other Information Technology Resources are not to be used for any illegal purpose including, but not limited to, illegal file sharing. Accordingly, to preserve network security and reliability, the College reserves the right in all instances, and upon its reasonable suspicion, to block access from and to its network of any IP address associated with illegal activity and/or to disconnect any User from the network who can be traced to illegal activities, including illegal P2P file sharing. An infringing User shall bear legal and financial responsibility for events or activities resulting from or associated with his/her own misuse of P2P applications and any other illegal activity conducted by or through the College's network.

8.2 Students. Faculty and Staff

In addition to barring access to network resources, a student, faculty or staff member who violates this Policy may also be subject to other appropriate discipline, up to and including termination of employment and/or expulsion. No final adverse action may be taken pursuant to this Section, however, with respect to any employee or student of the College unless such employee or student is afforded a meaningful opportunity to contest the adverse action, as further described in Section 9.0.

8.3 Contractors. Vendors. Consultants. Volunteers and Others.

Any party external to the College, including but not limited to, College contractors, consultants, or vendors found to have violated this Policy may be held in breach of contract and, in such event, may be subject to such sanctions and damages as may be allowed under the contract and/or applicable law including, but not limited to, ineligibility to be considered a responsible source for subsequent contracting with the College. Other parties who violate this Policy but who do not have a contractual relationship with the College (including volunteers) may be barred from any subsequent use of a College Information Technology Resource.

8.4 Criminal and Civil Liability; Reporting to Government Authorities

In addition to the actions described in Sections 8.1, 8.2, and 8.3, the unauthorized acquisition or distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject culpable individuals to civil and criminal liabilities. To the extent required by federal or state law, or when the College otherwise deems it to be in its best interest, the College will report certain illegal activities to designated law enforcement agencies without prior warning or notice to the infringing User.

9.0 ENFORCEMENT PROCEDURES FOR HANDLING UNAUTHORIZED P2P FILE SHARING

9.1 Alleged Violations

Alleged violations of the Digital Millennium Copyright Act (DMCA) shall be received by the IT's Designated Agent for the Receipt of a Claimed Infringement ("Designated Agent"). IT shall respond to all DMCA notices. The receipts of such notices are to be logged in and tracked by IT. Attempts to identify the suspect computer(s) and User(s) will be made by IT staff. In the case of suspected offenders who are students, if successful identification is made, a copy of the notice and name of student(s) identified shall be referred to the Office of the Dean of Students in accordance with Section 9.2(b). In the case of suspected faculty or staff who are successfully identified, the notice and name of the staff or faculty member(s) and relevant identifying information shall be referred to the employee's supervisor. In circumstances when criminal activity is suspected, the CIO shall consult with the Office of

Legal Affairs and the College Department of Public Safety before notifying any party.

9.2 Students

(a) Generally -- Disciplinary proceedings involving students alleged to have violated this Policy shall be conducted in accordance with those procedures specified in the Student Handbook.

(b) DMCA -- Violations of the DMCA by students shall be resolved as follows:

(1) Upon receipt of an alleged violation of the DCMA, the Designated Agent shall identify the person associated with the IP address cited in the Claim. If the identified person is a college student, IT shall notify the Office of the Dean of Students and the Office of Legal Affairs. The Office of the Dean of Students will notify the student of the claim. Students who receive such notices must respond to the Dean's notice within the period of time specified by the Dean of Students, but in no event later than 3 school days after the notice of claim is received by the student. Such students shall be requested to acknowledge the notice and state whether they have received their own copy of the DMCA claim. If this is a first offense and the student acknowledges a violation of this Policy by admitting to the claim, he/she will be asked to stipulate in writing that he/she will comply with this Policy in the future. If the Office of the Dean of Students does not receive such an acknowledgement and stipulation within the prescribed time period, or if the student challenges the validity of the claim, the Dean will initiate disciplinary proceedings.

(2) A second offense of this Policy will become a part of the student's disciplinary record.

(3) A third or fourth violation of this Policy will result in an automatic referral to the Honor Board through the Office of the Dean of Students. Sanctions may include fines and/or a disciplinary probation period or expulsion.

In any situation listed in (1) through (3) of this subsection, the College may suspend the rights of access to the College's network pursuant to Section 8.1 pending the final disposition of the disciplinary matter.

9.3 Faculty/Staff

Disciplinary proceedings involving faculty alleged to have violated this Policy shall be conducted as provided for in relevant provisions of the Faculty/Administration Manual. Disciplinary proceedings alleging violations of this Policy by staff shall be conducted in accordance with relevant provisions of controlling law and, to the extent applicable, the College's Code of Conduct and Disciplinary Actions and the College's Grievance Procedure. The College may suspend the rights of access to the College's network pursuant to Section 8.1 pending the final disposition of any employee disciplinary action.

9.4 Subpoena

The College will timely comply with all valid subpoenas seeking the identity of a person alleged to have misused the College's Information Technology Resources for illegal purposes.

10. ASSESSING EFFECTIVENESS

10.1 Assessment

Within 60 days after the effective date of this Policy, the Division of Information Technology will de-

velop relevant assessment criteria to periodically review and evaluate the effectiveness of the College's plans to prevent the unauthorized distribution of copyrighted materials by Users of the College's computer network. In gathering information for such assessment, the Division of Information Technology shall, among other things:

(a) add questions to such surveys distributed to students and employees as may be appropriate in an attempt to detect awareness levels of this Policy held by students and employees;

(b) review of reports annually reflecting utilization of the College Network for the downloading of large files; and

(c) track annually of the number of file sharing violations reported to the Division of Information Technology.

10.2 Reporting

Information gathered by IT pursuant to Section 10.1 shall be provided to the President's Executive Team by the CIO. In addition, the CIO shall publish the results of the assessment conducted pursuant to this Section 10.0 on its webpage relating to this Policy.

11. AMENDMENTS

This Policy may be amended in accordance with the College's Campus Wide Policy Making Procedures.

12. RESPONSIBILITY

The Chief Information Officer of the College and the Dean of Students shall be responsible for the maintenance of this Policy

13. EFFECTIVE DATE

This Policy shall become effective immediately and shall be fully implemented no later than July 1, 2010.