I. PURPOSE..... 1
II. POLICY..... 1
III. ENFORCEMENT..... 2

I. PURPOSE

The Digital Millennium Copyright Act of 1998 ("DMCA") legally protects a copyright holder from the unauthorized use of his or her digital content. Unauthorized use means violating the user agreement or terms of use for the digital content. Illegally sharing and/or reproducing copyrighted materials such as music, videos, documents, software, and photos is considered copyright infringement. The Higher Education Opportunity Act ("HEOA") includes a provision directly related to DMCA.

HEOA sets requirements for higher education institutions to address illegal peer-to-peer ("P2P") file sharing occurring on College networks. Illegal P2P file sharing is downloading, also known as copying and/or saving, copyrighted material to a hard drive or any other storage device and/or sharing or making it available to other people without the consent of the copyright holder.

P2P applications are used to legitimately share digital content. However, P2P applications can expose the College, and individual users on the College's network, to legal liabilities when illegal file sharing occurs. P2P applications can also present a security risk because a downloaded file may actually contain a virus or a malicious program that could target and infect other machines on the network, impact the performance of the network and compromise sensitive/confidential information.

The purpose of this Policy is to inform the College community on preventive measures that will help avoid legal liability and security risks resulting from illegal file sharing. This Policy applies to any individual using the College's computer network.

II. POLICY

Individuals using the College's computer network will be held accountable for adhering to the following terms and conditions:

- Read the user agreement or terms of use for the following digital content in order to make sure you do not use nor share digital material illegally: documents, videos, and games

located on the Internet; social networking sites (i.e., YouTube); purchased digital content (i.e., music, software); and peer-to-peer file sharing applications;
- Delete unauthorized copyrighted material from your electronic device (e.g., computer, iPhone);
- Use a legal alternative to unauthorized downloading. The College does not endorse a particular product or service nor is it responsible for any cost or any technology related issues resulting from the use of the legitimate sources;
- Disable the file sharing feature for P2P software if you do not have permission to share the digital material (i.e., documents, movies, games, etc.) legally; contact the software vendor for technical support;
- Follow the P2P vendor's best practices for securing the computer used for P2P activity (i.e., anti-virus software, a vendor supported operating system, personal firewall, current version of P2P application, etc.); the Federal Trade Commission has P2P best practices at: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm; and
- For College-owned assets, P2P software can only be used to promote the College's mission, academic and business needs. Where applicable, P2P software is not allowed on machines that process and/or store confidential/sensitive data. The personal use of P2P applications on College-owned assets is prohibited.

III. ENFORCEMENT

Enforcement of this Policy shall include:

- Monitoring network traffic and limiting network bandwidth; and
- Implementing other technology-based deterrents as needed.

In addition to employment and student discipline issued by the College in accordance with applicable policies and procedures (up to and including dismissal/suspension), individuals cited for unauthorized use may be subjected to civil and/or criminal damages such as monetary damages and potential prison time. According to the US Copyright Office, monetary damages can range from $200 to $150,000 for each act (http://www.copyright.gov/title17/92chap5.html#504). Criminal prosecutions may result in a fine of up to $250,000 and a prison term of up to 5 years (http://www.fbi.gov/ipr/) for each act.

REFERENCES

Statutory References	20 U.S.C. §§ 1092, 1094
Regulatory References	None
Relevant Guidance	None
Policy Manual Cross-References	None

POLICY HISTORY

September 12, 2023	Adopted.