POLICY ON PEER-TO-PEER FILE-SHARING AND COPYRIGHT INFRINGEMENT

Background

Peer-to-peer (P2P) file-sharing allows users to share files online through an informal network of computers running the same software. File-sharing can give access to a wealth of information, but it also has a number of risks. Those sharing files can inadvertently download copyright-protected material, pornography, or viruses or mistakenly allow other people to copy files not intended for sharing.

Copyright infringement is the use of works protected by copyright law without permission, thereby infringing on certain exclusive rights granted to the copyright holder, such as the right to reproduce, distribute, display, or perform the protected work or to make derivative works. The copyright holder is typically the work's creator or a publisher or other business to which copyright has been assigned. Copyright holders routinely invoke legal and technological measures to prevent and penalize copyright infringement.

Please refer to copyright law of the US and related laws contained in Title 17 of the *United States Code* (*http://copyright.gov/title17/92preface.html*).

Consequences a violator of copyright law might face include (but are not limited to) the impounding of equipment, legal fees, fines, and statutory damages. Any student, faculty member, administrator, or guest that knowingly violates copyright law does so at their own risk and in violation of this policy.

Manipal Education Americas, LLC (MEA) and the American University of Antigua will distribute, on an annual basis, a notification to the university community that illegal distribution of copyrighted materials may lead to civil and/or criminal penalties. In addition, the university will provide students with information on sites that provide safe and legal file-sharing options via continuous updates to the permitted activities section of this document.

Purpose

The purpose of this policy is to describe our shared responsibility to not expose the university to the security risks, liabilities, and the degradation of computing resources caused by P2P file-sharing and copyright infringement.

Scope

This policy applies to all university-supplied computers, laptops, tablets, servers, network appliances, and mobile devices. This policy also applies to any personally owned device that is connected to the university network. This policy applies to all individuals regardless of their university affiliation and/or status.

Policy

It is the policy of MEA and AUA to comply with copyright law.

This policy prohibits the distribution, downloading, or uploading of any content, software, data, sound, or picture that

- is copyrighted;
- is specified as illegal or forbidden to copy without the copyright owner's written permission;
- is considered to be proprietary or private; and
- contains viruses or malware.

P2P file-sharing is strictly forbidden

- from any university supplied computer, laptop, server, or mobile device;
- from any personally owned device connected to the university network.

Other forbidden activities include

- using BitTorrent (or any similar means) to download content that is not free for public use;
- running programs that attempt to conceal forbidden activities from university network security monitors;
- transmitting or downloading any material that infringes any patent, trademark, trade secret, or copyright; and
- downloading, installing, or distributing pirated or unlicensed software.

Permitted activities include

- using BitTorrent (or any similar means) to download software marked freely available by its owners; and
- downloading content, music files, documents, and pictures that the owner and/or artist have marked as freely available.

Enforcement

MEA and AUA will take steps to detect, suspend network access, and punish individuals that violate this policy.

The university has active network monitors in place that prohibit access to illegal file-sharing sites and alert the IT organization as to suspicious activity that warrants further investigation.

MEA and AUA consider any violation of this policy to be a serious offense. MEA and AUA reserve the right to copy and examine any files or information resident on MEA systems and to

protect its network from systems and events that threaten or degrade operations. Please note that violators are subject to disciplinary action that is consistent with the severity of the breach of policy, and in some cases violations may be reported to appropriate authorities for criminal or civil prosecution. Copyright status is applied to a work as soon as it is created. Users should assume that all writings and images are copyrighted.

ACCEPTABLE USE OF TECHNOLOGY

Our computers' email and information systems have been organized to improve communication and reduce the time and effort it takes to complete administrative activities. Use of university-supplied computers, email, and information systems must always reflect that these are shared resources that have been established for the good of AUA, LLC, and the university community.

The guidelines below reflect the commitment students are required to make to use university-supplied technology resources properly and responsibly.

In making acceptable use of resources you must do the following:
1. Protect your system username and password from unauthorized use.
2. Understand that you are responsible for all activities that originate from your system account.
3. Access only information that is your own, that is publicly available, or to which you have been given authorized access.
4. Use only legal versions of copyrighted software in compliance with vendor license requirements.
5. Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.
6. Use resources only for authorized purposes.

In making acceptable use of resources you must not do the following:
1. Use another person's computer, system name and password, or files.
2. Use computer programs to decode passwords or access control information.
3. Attempt to circumvent or subvert system or network security measures.
4. Engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files, or making unauthorized modifications to university data.
5. Use university systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political students.
6. Make or use illegal copies of copyrighted materials or software, store such copies on university systems, or transmit them over university networks.
7. Make disparaging comments about others or make statements, speak, or write on behalf of AUA in a newsgroup or chat room unless you are duly authorized to do so by the university.
8. The electronic mail system shall not be used to create, send, or receive any offensive or disruptive messages. Among those which are considered offensive include any messages that contain sexual implications, racial slurs, gender-specific comments, or any comments that offensively address someone's age, sexual orientation, religious or political beliefs, national origin,

or disability. Email communications should be considered official communications and should be composed in a professional, businesslike manner.
9. Use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or system username.
10. Waste computing resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
11. Use the university's systems or networks for personal gain, for example, by selling access to your system username or to university systems or networks, or by performing work for profit with university resources in a manner not authorized by the university.
12. Access content that is pornographic in nature.
13. Intentionally cause physical damage to a technology asset.
14. Engage in any other activity that doesn't comply with the general principles presented above.

Classroom Communications

The classroom is AUA University controlled space in which faculty and students communicate with each other and members of the public. There is no right to privacy regarding communications which takes place in such a setting. Any expectation to privacy concerning communications taking place in educational classrooms during classes or classroom related activities are subject to audio and video monitoring solely for educational purposes. By entering a classroom setting one acknowledges that they agree with and acknowledge the above.