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 you access to a wealth of information, but it also has a number of risks. You could download copyright-protected material, pornography, or viruses without meaning to or you could mistakenly allow other people to copy files you don't mean to share.

Copyright infringement is the use of works protected by copyright law without permission, infringing 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 United States of America 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, administrator or guest that knowingly violates copyright law does so at their own risk and in violation of this policy.

MEA LLC 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 resource caused by peer to peer 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 LLC and the American University of Antigua to comply with copyright law.

This policy prohibits the distribution, downloading or uploading of any content, software, data, sound and 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
- Contains viruses or malware

P2P file sharing is strictly forbidden:

- From any university supplied computer, laptop, server and or mobile device
- From any personally owned device connected to the University network

Other forbidden activities include:

- Using BitTorrent (or any similar site) 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
- Downloading, Installing or distributing pirated or unlicensed software

Permitted activities include:

- Using BitTorent (or any similar site) to download software marked freely available by its owners
- Downloading content, music files, documents and pictures that the owner and or artist have marked as freely available

Enforcement

MEA and the American University of Antigua 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 the American University of Antigua consider any violation of this policy to be a serious offense. MEA and the American University of Antigua 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. Your 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 the AUA, LLC and university community.

The guidelines below reflect the commitment you are required to make to use University supplied technology resources properly and responsibly.

In making acceptable use of resources you must:

1. Protect your system user name 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:

1. Use another person's computer, system name & 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, or 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 candidates.
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, LLC in a news group 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 which 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 business-like 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 user name.
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 user name 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 does not comply with the general principles presented above.