



## **2007 COPYRIGHT AND SECURITY GUIDE FOR SCHOOLS AND UNIVERSITIES<sup>®</sup>**

**ivf**  
International Video Federation

  
**MPA**<sup>®</sup>

  
representing the  
recording industry  
worldwide

Most academic institutions have policies in place to ensure the respect of copyright on their computer networks. This booklet provides simple and practical guidelines for University and College administrations to help them communicate, implement and enforce these policies for the benefit of copyright holders and the academic community.

## CONTENTS

- 03 **WHAT ARE THE RISKS?**
- 04 **WHAT TO LOOK OUT FOR**
- 05 **RESPECTING COPYRIGHT – SOME GUIDELINES**
- 06 **SAMPLE MEMO**
- 07 **SAMPLE CODE OF CONDUCT**



Copyright infringement is a legal, ethical and security issue for academic institutions.



## WHAT ARE THE RISKS?

Copyright law prohibits the copying and distribution of music and films on the internet via computer systems, without permission from the copyright owner. As generators of intellectual property, academic institutions will understand the importance of protecting copyrighted material. They are also well-placed to communicate about this issue with young adults.

For colleges and universities, copyright infringement is also a computer security issue. Without adequate precautions, their systems can easily be abused by internal users or external hackers, becoming illegal distribution engines for copyrighted material. This raises a number of legal and security risks for an institution, its staff and students.

This guide aims to help academic institutions ensure that their computer network remains free of pirated material and protected from legal and security risks.

### CIVIL OR CRIMINAL LAWSUITS

The laws of virtually every country make it both a civil and a criminal offence to make illicit copies, distribute and/or make available a third party's material on the internet without their permission. Copyright owners are particularly concerned about copyright theft using academic and public networks, given the speed and scale of damage that can result. Most academic institutions set out rules that encourage responsible use of their computer networks and warn against infringing copyright. Unfortunately, these may often not be enforced in practice. This can result in legal action not only against students, but also against academic institutions whose systems are hosting databases of infringing copyright material, acting as a hub for its distribution or facilitating illegal copying or "file-sharing".

### SECURITY BREACHES

A system hosting peer-to-peer (P2P) software may be running serious risks to its data, confidentiality and IT security. Illegal websites including forums, blogs and newsgroups and unlicensed file-sharing services are the source of much illegal music, film, software and other copyright material. They are notorious sources of the following:



**Viruses** can crash individual machines, destroy the contents of computers and file servers, compromise infrastructure security and spread throughout a network. This is especially likely if an institution allows users to connect to its network with their own computers which typically may not have a robust anti-virus protection setup.



**Spyware.** Filesharing software often includes 'spyware' or 'adware' that reports on computer usage, delivers advertising or other unsolicited files which is resource draining and can be difficult or damaging to remove.



**Firewall compromise.** Many P2P systems offer users advice on how to adjust firewall settings so as to open up 'holes' needed for P2P systems to connect to each other. These also represent a means for viruses and worms to bypass the protection offered by a firewall.



**Resource drains.** Unlicensed music film and other copyright files can eat up gigabytes on a server and in PC hard disk space, increasing an institution's storage costs. File-sharing typically consumes a high proportion of an academic institution's network and internet bandwidth, denying access for legitimate users and reducing academic productivity.



**Hacking.** Academic computer resources are sometimes hacked by insiders or outsiders to access personal files and content or establish copyright-infringing music distribution services. This can range from simply placing music files onto a public website, to hacking servers whose unused ports and services have not been sufficiently locked down.

One or more of the following signs indicate a need to act on copyright abuse:

## WHAT TO LOOK OUT FOR

- 
- Staff and students show little awareness of regulations.** Many colleges and universities lack a comprehensive policy that makes clear what practices are, and are not, acceptable on their network. Others have such policies, but do not communicate them effectively. Institutions should explain clearly and on a regular basis to students and staff what their rules are, and outline disciplinary steps for those that break them. They should also appoint a compliance officer.
  - There are no technical systems in place to enforce policies.** There are an increasing number of technical measures available that help curb illegal or unwanted activity on IT networks. Installing these could help an institution reduce risks and save costs.
  - Systems administrators see evidence of large amounts of files being traded on their networks.** Many education institutions already take an inventory of copyrighted material on all of their networks and computers. Administrators should check their institution's servers and PCs for caches of copyrighted material unrelated to their institution's function or legitimate academic use. Technical staff should also check whether users have installed file-sharing software without their institution's permission.
  - Internet and network connections are very slow.** Poor network response times may indicate internal 'bandwidth hogs' or unwanted traffic from file-sharing services. It may also signal viruses, spyware or other destructive elements associated with unauthorised P2P programmes.
  - There are regular problems with computer viruses.** If systems and computers have been plagued with viruses it may be that users are accessing sites or services offering illegal copyright material. Viruses may also be transmitted by less well-protected computers that have access to the network's resources.
  - There is no internet firewall or unauthorised traffic is present on an internet connection.** To stop intruders and unauthorised outbound activities, every institution on the internet should have a properly configured firewall. Inbound and outbound rules on internet equipment should be set to block ports and protocols that are commonly misused. Universities should ensure that wireless (e.g. WiFi or WiMax) connections are secure and that access is restricted to authorised users.

## Colleges and universities can take steps to curb copyright infringement on their networks.



# RESPECTING COPYRIGHT – SOME GUIDELINES

## 1 SET A COPYRIGHT POLICY AND COMMUNICATE IT.

Staff and students should understand that illicit copying and transmission of someone else's music, film or other works is copyright abuse, which the university does not condone and which carries legal and financial penalties. This is best implemented in a code of conduct and terms and conditions of enrolment. In the UK, the policy that defines who may connect to and use JANET (Joint Academic NETWORK of UK education) is maintained by JISC (Joint Information Systems Committee) and is a useful model.

Go to [www.ukema.ac.uk/services/publications/policy/aup.html](http://www.ukema.ac.uk/services/publications/policy/aup.html)

Your policy should spell out unacceptable behaviour on academic networks in classrooms, campus and in dorms, including illegal file-sharing, and make clear the penalties. A sample memo and code of conduct provision are at the back of this booklet.

It should be well communicated to staff and students by taking simple steps, for example:

- Making the policy available right from enrolment in the form of brochures and flyers in freshers' packs. It should also be easily available on its website.
- Ensuring that students sign a document agreeing to these terms before being allowed access to the computer network.
- Sending periodic reminder emails directly from senior figures in the institution.

## 2 CHECK WHAT IS ON THE SYSTEM.

Many institutions already audit their systems for certain types of copyrighted material, particularly software. Inventories should also include music, film and other major types of copyrighted works. Music files are typically three to five megabytes in size, stored in .mp3, .wma, .ogg, .flac or .wav formats and found in \my music or \shared directories. Increasingly, music files are also distributed as complete albums and stored in .zip [or .rar] format. Movie files are typically 500 to 700 megabytes in size, stored in .avi, .mpg or .mov format. These files can sometimes be included in compressed files like .zip or .rar files.

## 3 DELETE COPYRIGHT INFRINGING MATERIAL.

Institutions should check that any copies of commercial music on their systems are legal. 'Private copy', 'academic use', 'fair use', 'evaluation copy' or other such excuses do not permit the storage or transmission of libraries of commercial recordings on academic institutions' systems.

## 4 CONTROL FILE-SHARING.

Banning unauthorised software installations and file-sharing activity on a university's system is one way of reducing copyright and security problems, stopping the vast majority of copyright piracy before it takes place. There are also technologies which can help academic institutions tackle copyright misuse. For example, one network-based system developed by Red Lambda is cGrid ([www.redlambda.com/Products\\_overview.htm](http://www.redlambda.com/Products_overview.htm)), pioneered by the University of Florida in the US.

It can be customised by a university to provide selective or complete blocking and also addresses a full range of other security management issues.

Another option is to install a network filtering system. Unlicensed copyrighted recordings can be identified within peer-to-peer traffic and individually blocked, while leaving other peer-to-peer traffic unaffected. Audible Magic's "Copysense" application ([www.audiblemagic.com](http://www.audiblemagic.com)) is one such technology.

## 5 SET FIREWALL RULES.

Firewalls can also be useful tools to restrict excessive P2P bandwidth usage. Particular internet addresses, ports or protocols on which file-sharing typically occurs can be blocked. Best security practice is to lock down all ports at the firewall that are not specifically needed for authorised internet activity. Sophisticated software that can selectively filter or block copyrighted material as it passes from the internet to an institution's local infrastructure is also available. Many institutions are installing such programmes as a matter of course alongside the filters they would use to block viruses, spyware/adware and malicious e-mails.

## 6 CONTROL WIRELESS ACCESS.

Academic institutions should be sure that wireless connections to their network and the internet are secured and encrypted, so that these connections are not hijacked for illegal purposes. Wireless hub software lets organisations set access codes and the desired level of encryption.

## 7 WATCH TRAFFIC LEVELS.

Network monitoring software, which may have been supplied with network equipment, allows institutions to check whether users or devices are hogging bandwidth and if configured to do so can automatically ban users from a network on a temporary or permanent basis. Technical staff should check traffic 'hot spots' to see if there is a system problem or illegal activity taking place.

## 8 MAINTAIN VIRUS PROTECTION.

Anti-virus software can screen out rogue files containing viruses, spyware or other damaging material, and should be installed on every computer. Vendors update this software regularly to take account of new viruses. Institutions should be sure that all copies of anti-virus programmes are run regularly and kept up to date.

## 9 MAINTAIN SPYWARE PROTECTION.

There are software programmes which can find and remove spyware, adware and similar programmes from an institution's machines. Anti-spyware programmes should be run and updated regularly.

## 10 DESIGNATE A COMPLIANCE OFFICER.

Someone within each institution should be responsible for ensuring copyright compliance. The person needs to be sufficiently senior (such as the IT or finance director) to insist on ongoing compliance with the institution's code of conduct, to remove illicit material promptly and to deal with notices or disciplinary actions should they arise.

# SAMPLE MEMO

You can download a copy of the following memo and policy from [www.ifpi.org](http://www.ifpi.org)

## MEMO

TO: (DISTRIBUTION LIST)

FROM: (HEAD OF THE INSTITUTION)

SUBJECT: CODE OF CONDUCT ON THE USE OF COPYRIGHT MATERIAL

DATE: (INSERT)

(Institution) takes a very serious view of its computer networks being misused to infringe copyright.

The purpose of this letter is to remind you of (Institution)'s policy on the use of copyright material on (Institution's) computers, networks and media.

Unless you have the copyright owner's permission, transmitting copyrighted material (including over the internet) and copying such material in any way other than for legitimate academic or personal use, is illegal and can expose you and (Institution) to civil and criminal liability under copyright law. This applies to all types of copyright material, including music, films, games, software and other works.

Individuals caught illegally transmitting copyrighted materials have faced legal action and had to pay thousands of [pounds/euros/dollars] in compensation.

Staff and students must not put unauthorised copies of copyrighted material on computers, networks or media owned by (Institution).

Nor should they put unauthorised copyrighted material on the internet, or engage in activities such as peer-to-peer 'file-sharing' that are likely to promote or lead to copyright infringements.

(Institution's) detailed policy on the use of copyright material, which includes possible disciplinary actions for failure to abide by this policy, is attached. (Compliance Officer) is charged with ensuring compliance and removing illicit items if you have not done so.

Contravening this policy will result in disciplinary action and you may be prohibited from using (institution's) computer networks.

Please do not hesitate to contact (Compliance Officer) if you have any questions.



# SAMPLE CODE OF CONDUCT

This code of conduct should be a clearly explained part of a college's IT policy.

For an example see the "Guidelines For Internet Use" and "Acceptable Use Policy" set out by Wolfson College on [www.wolfson.cam.ac.uk/facilities/computers/netuse/](http://www.wolfson.cam.ac.uk/facilities/computers/netuse/)

## POLICY ON THE USE OF COPYRIGHT MATERIAL

(Institution) takes very seriously the need to respect the copyright of those involved in creating and disseminating copyright material, such as music, films, software and other literary, artistic and scientific works.

It is also concerned that the misuse of your computer or (Institution's) network could get you into trouble with the law, or create security breaches which might affect your work and that of your fellow students and teachers.

This is why (Institution) has created a set of rules that you are required to adhere to in order to connect to the network.

### **(Institution) staff and students may not:**

- make, store, transmit or make available copies of copyright material on (Institution) systems, equipment or storage media, unless they have obtained express prior written authorisation from the relevant copyright owner(s).
- upload, store or make available unauthorised copies of copyright material via the (Institution) local area network or the internet using (Institution) systems, equipment or storage media, unless they have obtained express prior written authorisation from the relevant copyright owner(s).
- assist or participate in any infringement of copyright by operating or connecting to a peer-to-peer 'file-sharing' network, or operating a peer-to-peer index or server, using (Institution) systems or equipment on school grounds or dormitories.

(Compliance Officer) is responsible for carrying out this policy. The only exception to the above rules is the use by staff of copyright material strictly for [educational purposes] in accordance within the limits permitted by copyright law.

Any questions as to whether a student or member of staff may copy or use copyrighted material in ways covered by this policy should be raised with (Compliance Officer) before proceeding.

(Institution) staff and students that contravene this policy will be subject to temporary or permanent disconnection of their IP address [and/or network socket]. They will be charged for any costs incurred by (Institution) and may be subject to disciplinary procedures, which could include a permanent ban on the use of (Institution's) computer facilities and network.

Any activities or materials that violate this policy are subject to immediate removal.

---

Signature and date



representing the  
recording industry  
worldwide



International Video Federation

IFPI  
10 Piccadilly  
London  
W1J 0DD  
United Kingdom

Tel: +44 (0)20 7878 7900  
Fax: +44 (0)20 7878 7950  
[www.ifpi.org](http://www.ifpi.org)

Motion Picture Association  
European Office  
Rue Du Trone, 108  
B-1050 Brussels  
Belgium

Tel: +32 (0) 2 778 2711  
Fax: +32 (0) 2 778 2700  
[www.mpaa.org](http://www.mpaa.org)

International Video Federation  
38 Avenue des Arts  
B-1040 Brussels  
Belgium

Tel: +32 (0) 2 503 40 63  
Fax: +32 (0) 2 503 37 19  
[www.ivf-video.org](http://www.ivf-video.org)