



representing the
recording industry
worldwide

COPYRIGHT USE AND SECURITY GUIDE for academic institutions



INTRODUCTION



All of the people that create music rely on a fair reward for their creativity, their time and their hard work to keep doing what they do. In the case of those involved in creating commercially produced music, their fair reward depends on people buying rather than stealing music – the latest form of which involves mass copying and transmission of music over the internet without the permission of those who created it.

Unfortunately, students and other users of academic institutions' computers and networks sometimes use the institution's systems to distribute commercially produced music over the internet, or to copy music files in ways other than for legitimate academic or personal use. This not only wastes the institution's system resources, it is illegal.

Tolerating copyright theft increases security and privacy risks on your systems, and puts both users and your institution at risk of legal prosecution. It also sends exactly the wrong message about responsible use of other people's material to students who are expected to avoid plagiarism in their academic work, and who will face serious consequences in public or private sector jobs if they engage in copyright theft.

This brochure explains the problem of copyright theft in the academic environment, what can be done about it, and how you can implement policies to minimise the risk to your institution and the users of your computer systems. Copyright theft is bad business for everyone!

Jason Berman
Chairman and Chief Executive Officer
IFPI - representing the recording industry worldwide

WHAT ARE THE RISKS?

Unauthorised copies of copyright material like music on your computers pose legal and security risks.

Copyright material is someone else's property. When you or users of your institution's computers or networks copy and make available someone else's music on these systems without permission from the copyright owner, it is not 'sharing', 'academic freedom' or 'fair use'. It is copyright theft.

When these works are transmitted indiscriminately to others on the institution's local area network or over the internet, it is no different from running an illegal distribution business. Needless to say, illegal copying and transmission of copyright material also raise security risks from rogue files and firewall breaches.

Legal risks include injunctions, damages, costs, and possible criminal sanctions against the institution and its users.

Copyright encourages people to develop creative works like music, and protects the livelihood of everyone involved in making it. The laws of virtually every country therefore make copyright theft both a civil and a criminal offence to protect this important cultural and economic activity.

Copyright owners and law enforcement officials regularly take legal action against people and institutions that violate copyright using computer systems. In several countries, this has included academic users and institutions copying and transmitting substantial quantities of commercial music files in mp3 or other formats on their systems.

Most academic institutions have co-operated fully with copyright owners in removing unauthorised materials when found. And a number have already implemented codes of conduct specifying the institution's expectations regarding responsible use of copyright materials.

Copying and transmitting illicit copies of copyright material like music also raise security and other risks for your computers and networks.

- **Viruses, trojan horses, and other destructive elements.** Unauthorised files purporting to be music or other copyright material in many cases may not be what they claim. They may harbour rogue programs, links or scripts that pose a risk of damage to your systems.
- **Spyware.** Some peer-to-peer software includes undocumented 'spyware' that reports on computer usage, delivers advertising and other unsolicited files, and prevents its removal without substantial time and in some cases computer damage.
- **Firewall breaches.** Peer-to-peer file transfer programs in particular may demand an open port (1214, 6346, 6347, 6666, 6699, 7777, 8888 or other port) between the user's computer and the public network. This is nothing less than a hole in the firewall that you are using for network security.
- **Bandwidth and resource hogs.** Unauthorised music files also can eat up gigabytes of your server and PC hard disc space. Unauthorised downloading, uploading and indexing (such as on illicit peer-to-peer services) can affect network and internet bandwidth dramatically.

WHAT CAN BE DONE?

Set a clear policy against copyright theft.

Users, staff and IT personnel need to understand that transmission or illicit copying of someone else's music or other copyright material is not legitimate academic use but copyright theft, which your institution does not condone.

This is best implemented in your institution's **code of conduct and terms and conditions of employment**. A sample memorandum and code of conduct are attached.

Be aware of copyright material on your systems.

Many institutions already do regular audits of their systems for certain types of copyright material, such as software. Institutions also should check regularly whether their systems are being used for **illicit storage or transmission of other kinds of copyright material, including music**.

Music files typically are stored on computers in **.mp3**, **.wma** or **.wav** format. A typical compressed commercial recording takes up **3-5 megabytes**, and is often found in a **\my music** or **\shared** directory.

Delete unauthorised copies of copyright material.

Commercial recordings of music are virtually never licensed for multiple copying, network storage or distribution, or internet distribution, except by a recognised, legitimate music service or under an explicit licence agreement with the rights owner.

'Private copy', 'academic use', 'fair use', 'evaluation copy' or other such excuses do not apply to this kind of transmission and indiscriminate copying of music without rightholder permission. You should ask for and keep evidence to show that copies of commercially produced music on your systems are legal.

Take security precautions against further violations.

A range of technical precautions are available for academic institutions to reduce the risk of illegal copying of copyright material. These include:

- **Firewall configuration:** Your institution's internet firewall can be configured to screen out infringing files and illicit services.
- **Port scanning:** Software applications are available that detect attempts to run or join a peer-to-peer file transfer service, the source of much illegal material and activity.
- **Virus protection:** Up-to-date anti-virus software can screen out rogue files containing viruses, spyware or other damaging material.
- **Automatic inventories:** Commercially available software is available for maintaining a rolling inventory of installed applications and files.

Designate an appropriate copyright compliance officer.

Someone within your institution should be responsible for protecting against copyright theft on your systems. In many institutions, the IT or finance director is given this responsibility. The person needs to be sufficiently senior to insist upon ongoing compliance with your institution's policy, to take prompt action to remove illicit material, and to deal with notices and disciplinary actions should they arise.

MEMO

TO: (Distribution list)
FROM: (Senior Management Official)
SUBJECT: Code of Conduct on Use of Copyright Material
DATE: (Insert)

The purpose of this memorandum 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 copyright 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 the copyright law. This applies to all types of copyright material, including music, films, software and other literary and artistic works.

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

Nor should they put copyright material on the internet without permission from the copyright owner, or engage in activities such as peer-to-peer file indexing or transmissions that are likely to promote or lead to infringements of the copyright in this material.

(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 with this policy and, if necessary, removing unauthorised items if you have not done so.

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

POLICY ON THE USE OF COPYRIGHT MATERIAL

(Institution) respects the copyright of those involved in creating and disseminating copyright material, such as music, films, software, and other literary and artistic works created by others.

(Institution) staff and students shall not make, store, transmit or make available illicit unauthorised copies of such copyright material on (Institution) systems, equipment or storage media.

(Institution) staff and students shall not 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.

(Institution) staff and students shall not assist or participate in any infringement of such copyright materials by operating or connecting to a peer-to-peer network or index, using (Institution's) systems or equipment.

(Compliance Officer) is responsible for carrying out this policy. Any doubts concerning whether a member of staff or student may copy or use copyright material in ways covered by this policy should be raised with (Compliance Officer) before proceeding.

Any activities or material that violate this policy are subject to immediate removal, termination and/or forfeiture.

(Institution) staff and students that violate this policy are subject to discipline as appropriate under the circumstances. Such discipline may include suspension or dismissal.

Signature and date





IFPI Secretariat
54 Regent Street
London W1B 5RE
Tel: + 44 (0)20 7878 7900
Fax: + 44 (0)20 7878 7950
E-mail: info@ifpi.org
Web: www.ifpi.org