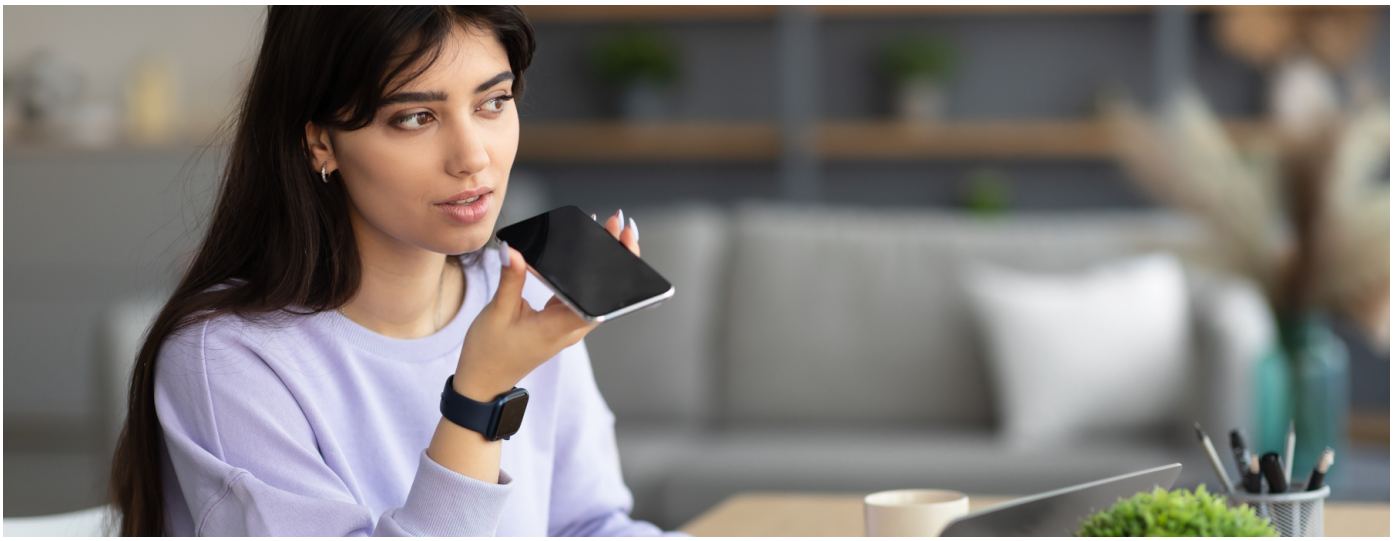
A-Z Guide

ILLEGAL FILE SHARING



Contents

Contents	1
Overview	2
Introduction	2
Copyright Act 1994	2
Copyright Infringing File Sharing Regime	3
Impact on Employers	5
Best Practice	6

Overview

The Copyright (Infringing File Sharing) Amendment Act 2011 altered the Copyright Act 1994, to provide a regime for copyright owners to enforce their rights against infringing file sharers.

Internet Service Providers can issue infringement notices to alleged infringers - those participating in illegal file sharing of copyrighted material. The internet account holder will be issued the notice. If the account holder continues to infringe after the third notice, the copyright owner could pursue an order from the Copyright Tribunal for a sum up to $15,000, and/or from the District Court to suspend the account holder's internet for up to 6 months.

Enforcement is against the internet account holder and not necessarily the individual user on the network. Therefore, employers should closely monitor their employee's internet usage in the workplace. Employers can challenge an infringement notice by writing in a prescribed form to their internet service provider.

Introduction

This **A-Z Guide** focuses on the Copyright (Infringing File Sharing) Amendment Act 2011 ("the Amendment"). This inserted new provisions, sections 122A to 122, into the Copyright Act 1994. The purpose of the Amendment was to provide a mechanism under which copyright owners could enforce their rights, against those involved in unauthorised sharing through the internet, of material subject to the owner's copyright.

The Amendment places an obligation on Internet Service Providers (IPAPs) to provided alleged infringers with infringement notices. The alleged copyright infringer will receive three notices prior to an action being taken in the Copyright Tribunal or the District Court. Continued infringement after the third notice has been issued may result in the internet account holder being ordered to pay a sum of up to $15,000 by the Copyright Tribunal, and an order to suspend the internet account holder's internet for up to 6 months.

Employers should closely monitor the use of their internet network in the workplace. Employers will generally be the internet account holder in their business, therefore, there is the potential for the employer be held personally liable.

Copyright

Under the Copyright Act 1994, the owner of a copyright has the exclusive right to copy or make an adaptation of the piece of work they hold a copyright in. They also have the exclusive right to issue copies of the work to the public; to play, perform or show the work in public; and communicate the work to the public. The Act calls these "restricted acts". A copyrighted work is infringed if any person other than the copyright owner or licence holder does any of these restricted acts. In the Act, the "doing of a restricted act" includes whether it is whole or part of the work, and whether done directly or indirectly.

Copyright infringing file sharing regime

Definitions

These are central to understanding the Copyright Act 1994 and its Amendment. They are from section 122A.

Account Holder	(In relation to an **IPAP**) A person who has an account with the **IPAP**
Detection Notice	The specific notice issued by an **IPAP** to an **account holder** in respect of *an* alleged **infringement** against a rights owner
Enforcement Notice	The specific notice issued by an **IPAP** to an **account holder** in respect of *at least 3* alleged **infringements** against a rights owner
File sharing	Circumstances where material is uploaded via, or downloaded from, the internet; and shared through an application or network with other users
Infringement	An incident of **file sharing** that involves the infringement of copyright in a work by the person engaging in file sharing
Infringement Notice	A **detection notice**, **warning notice**, or **enforcement notice** that is issued to an **account holder** by an **IPAP** and identifies a particular **infringement** that triggers the notice. In the case of a warning notice or an enforcement notice, it identifies any other infringements that have occurred since the date of the detection notice
IP address	**I**nternet **P**rotocol address - a number assigned to internet account holders by their internet service provider
IPAP	**I**nternet **P**rotocol **A**ddress **P**roviders. The Act refers to IPAPs rather than internet service providers, in order to only include traditional providers and exclude universities, libraries and businesses that provide internet.
On-notice period	A period of *28* days beginning on the date that the **detection or warning notice** is sent. During the on-notice period, the account holder will not be sent another infringement notice.
Quarantine period	A period of *35* days beginning on the date of the **enforcement notice**. The copyright owner has until the expiry of the quarantine period to bring enforcement action against the account holder. When the quarantine period ends, the enforcement notice alongside any preceding detection or warning notices expire.
Warning Notice	The specific notice issued by an **IPAP** to an **account holder** in respect of *at least 2* alleged **infringements** against a rights owner

Process

1. The copyright owner obtains the IP address of the alleged infringer (the user alleged to be participating in infringing file sharing of their copyrighted work). They have 21 days from the date of the alleged infringement to send the IP address.
2. The IPAP matches that IP address with the account holder (the one who was allotted the IP address when the alleged infringement occurred).
3. The IPAP sends the account holder an *infringement notice* within 7 days of receiving the information.
    - Where there are multiple instances of infringing, the infringement notice must identify the specific infringement that triggered the notice, which is the earliest recorded infringement.
    - The type of notice sent depends which number it is.

Notices

These are sent by the means the IPAP communicates with for billing purposes, unless the parties agreed in writing to use a different method.

First notice: *Detection* notice

Valid for 9 months or until the expiry of a following enforcement notice. The detection notice will:

- Identify the rights owner
- Identify the alleged infringement that has triggered the issue of the notice
- Identify the date of that alleged infringement
- State the date of the detection notice
- Explain the consequences to the account holder if further infringing occurs
- Explain how the account holder may challenge the notice
- Comply with any other requirements that may be prescribed in regulations

Second notice: *Warning* notice

Sent when the IPAP receives an allegation of further infringing, which must occur after the *on-notice period* (below) and before the *expiry* of the detection notice. The warning notice expires 9 months after the date of the detection notice or when a following enforcement notice expires. The warning notice will:

- Identify the rights owner
- Identify the infringement that has triggered the issue of the warning notice
- Identify the date of that alleged infringement
- Identify the most recent detection notice issued to the account holder, in relation to this rights owner ("the preceding detection notice")
- Identify any other alleged infringements, by the account holder against that rights owner, that have occurred since the date of the preceding detection notice
- State the date of the warning notice
- Explain the consequences to the account holder if further infringing occurs
- Explain how the account holder may challenge the notice
- Comply with any other requirements that may be prescribed in regulations

After these notices, there is a 28-day 'on notice' period. During this, any further incidents of infringement do not result in another infringement notice, although they are recorded.

Third and final notice: *Enforcement* notice

The final notice IPAP sends before a copyright owner can bring an action against an infringer. When sent to an account holder the IPAP also sends a copy to the copyright owner.

This is sent when the IPAP receives an allegation of further infringing after a *warning notice.* The infringement must occur after the *on-notice period* and before the *expiry* of the warning notice.

The enforcement notice expires 35 days after it is issued. When it expires, the preceding detection and warning notices do too.

The enforcement notice will:

- Identify the rights owner
- Identify the infringement that has triggered the issue of the enforcement notice
- Identify the date of that alleged infringement
- Identify the most recent warning notice issued to the account holder, in relation to this rights owner; and the preceding detection notice
- Identify any other alleged infringements against the rights owner that have occurred since the date of the preceding detection notice
- State the date of the enforcement notice
- Explain that enforcement action may now be taken against the account holder
- Explain that, unless the enforcement notice is cancelled, no further infringement notices may be issued in respect of infringements against the rights owner until the end of the quarantine period
- Explain how the account holder may challenge the notice
- Comply with any other requirements that may be prescribed in regulations

Penalties

After the third notice is issued, if alleged infringement continues, the copyright owner can seek enforcement against the account holder, by seeking an order from the Copyright Tribunal for a sum of up to $15,000, and/or an order from the District Court to suspend the account holder's internet for up to six months.

There are provisions in the Act for challenging any notices. However, the account holder is the liable party, whether or not they were the person who downloaded or uploaded the infringing file. The account holder will get infringement notices and be fined by the Copyright Tribunal.

Exceptions

The IPAP is not required to match an IP address to an account holder, if the alleged infringement occurred more than 21 days before the IPAP received the relevant information, or occurred during a quarantine period.

There is also a 28-day on-notice period between sending detection or warning notices.

If either of these apply - that there is no obligation to match the IP address with an account holder, or the account holder is on an on-notice period - the IPAP is not required to send out an infringement notice.

Challenging an infringement notice

An internet account holder that receives an infringement notice has 14 days from the date of the notice to challenge its validity. The challenge is forwarded by the IPAP to the copyright owner to consider. The copyright owner may either accept or reject the challenge. If rejected, the copyright owner must notify the IPAP, who then notifies the account holder of the rejection.

The copyright owner has 28 days to respond to the challenge. If the copyright owner fails to respond to the challenge within 28 days (from the date of the infringement notice), the challenge is deemed to have been accepted by the copyright owner.

If the challenge is accepted or deemed to be, that notice is cancelled and treated as if it was not sent. Any preceding notices may remain valid.

Impact on employers

Businesses should inform those using their internet that illegal file sharing will not be tolerated. You can update your workplace policy so clear guidelines are in place around the monitoring of internet usage. Policies need to state the steps that will be taken, including disciplinary action, in the case of alleged file sharing infringement by an employee. For more information about Discipline please refer to our **A-Z Guide** on **Discipline**.

Copyright owners who are concerned about the illegal sharing of their copyrighted material should consider developing an internal process to track the IP addresses of those sharing the copyrighted material.

In the workplace

Employers should be aware of what constitutes copyrighted material and the implications if an employer and/or their employees engage in file sharing. Works fall into two categories.

Authorised Copies

Works that the employer, company or employee are authorised to hold a copy of.

Employers should make sure that they have the authority to *retain* any copyrighted material that has been downloaded on work computers. Employers should also have authority over material that is *uploaded* onto the internet. Without the requisite authorisation, any copying or distribution of materials may amount to infringement. It is important that employees seek authorisation before using, copying or distributing any material that is copyrighted.

Employers should develop a policy to inform employees about copyrights and to manage the use and distribution of copyrighted materials. If you receive an infringement notice, or evidence that there has been illegal file sharing on the network, it is important that you can identify who the infringer was, on which computer, and how it happened, to avoid further infringement. Clear guidelines should be developed to reduce your risk of infringing a copyright.

Unauthorised copies

Any uploading or downloading of unauthorised copies of copyrighted material on the workplace internet may result in the internet account holder receiving a warning. There are some preventative measures that employers could consider using. It is possible to develop a policy that makes any non-work-related downloading serious misconduct.

Contractors and guests

Employers may be held liable for any infringing file sharing on their internet network. This will include infringements by contractors or other persons accessing your internet service. Employers must consider how their internet is used and by whom. With this in mind, employers should then consider the preventative measures required to limit the risk of infringing file sharing occurring on the workplace internet network.

Preventative measures

Options available to employers to reduce the risk of infringing file sharing:

- Using Proxy Servers or filtering methods, to reduce access to web sites that might allow downloading of copyrighted materials/music/video or software
- Removing access to websites not needed for the purpose of engaging in the company's business
- Using of administration rights to restrict adding peer-to-peer software on work or connected machines
- Advising, through notices on work computers, that internet access is subject to company rules and/or monitoring
- Making sure your virus protection is up to date
- Password protecting your wireless internet, so that only authorised users can access the internet

In the absence of an internal IT team, an IT contractor can manage preventative measures. To discuss preventative measures in more detail, employers should contact an IT specialist and their internet service provider.

Privacy

Employees are entitled to expect that their employers will preserve their right to individual privacy, and that they will be treated fairly. However, your organisation has a right to prescribe standards of conduct regarding people, the workplace and its tools. This includes monitoring employee activity on your computer and internet network, to prevent illegal file sharing. For more information about privacy please refer to the **A-Z Guide** on **Privacy**.

Best Practice

Employers are encouraged to ensure their computer and internet usage policy encompasses prohibition of illegal downloading. The policy should include what is prohibited use of the company's computers and internet network, and how usage will be monitored. It should provide a guideline of your organisation's investigatory and disciplinary processes, and the consequences of breaching the policy. The policy should be enforced consistently. For more information about creating and enforcing an internet and computer usage policy, please refer to the **A-Z Guide** on **Information & Communications Technology Policies**.

Employers should be sufficiently equipped and prepared to administer the computer and internet use policy, which includes developing methods of monitoring their employees' internet usage. Employers should also consider educating staff as to what amounts to illegal downloading and how to prevent the distribution of copyrighted materials.

Employers should monitor their emails, which are commonly the method through which internet account holders are billed, and therefore will be the method of communicating infringement notices. If you are concerned about not receiving infringement notices that have been sent, you should contact your IPAP to discuss delivering the notices through an alternative means.

The EMA has template and tailored options available for you to attain a computer and internet usage policy. Please contact the AdviceLine on 0800 300 362 for more information.

Remember

- Always call AdviceLine on 0800 300 362 to check you have the latest guide.
- Never hesitate to ask AdviceLine for help in interpreting and applying this guide to your situation.
- Use our AdviceLine employment advisors as a sounding board to test your views.
- Get one of our consultants to draft an agreement template that's tailor-made for your business.

This guide is not comprehensive and should not be used as a substitute for professional advice.

Published: **July 2024**

ema.co.nz | 0800 300 362