



A-Z OF EMPLOYING

Illegal File Sharing

Our guide for Employers and Managers

**SUPPORTING,
FACILITATING &
REPRESENTING
BUSINESS**

Business**Central** 

Illegal File Sharing

Our guide for Employers and Managers

Contents

This is only a guide.
It should not be a
substitute for
professional advice.

Please seek advice
from our AdviceLine
Team if you require
specific assistance.

Overview	3
Introduction	3
Copyright Act 1994	3
Copyright Infringing File Sharing Regime.....	4
Definitions	4
Overview.....	5
Notices	5
Penalties	6
Exception	6
Challenging an infringement notice	7
Impact on Employers.....	7
Copyright owners.....	7
In the workplace	7
Privacy	9
Best Practice	9

Illegal File Sharing

Our guide for Employers and Managers

Overview

The Copyright (Infringing File Sharing) Amendment Act 2011 came into force on 1 September 2011. Sections 122A to 122U of the Copyright Act 1994 provides a regime through which copyright owners can seek enforcement of their rights against infringing file sharers.

Under the regime, infringement notices can be issued by Internet Service Providers to alleged infringers who are participating in illegal file sharing of copyrighted material. The internet account holder will be issued with 3 infringement notices. After the 3rd notice is issued, if the account holder continues to infringe, the copyright owner could pursue an order from the Copyright Tribunal for a sum up to \$15,000 and / or an order from the District Court to suspend the account holder's internet for up to 6 months.

Enforcement is against the internet account holder, not necessarily the particular 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 addresses the Copyright (Infringing File Sharing) Amendment Act 2011. The provisions of the Act were inserted into the Copyright Act 1994.

The purpose of the Act was to provide a mechanism under which copyright owners could enforce their rights against those involved in the unauthorised sharing of material that was subject to their copyright via the internet. Prior to the enactment of the Copyright (Infringing File Sharing) Amendment Act 2011, a copyright owner did have the ability to sue for damages under the Copyright Act 1994.

The Act places an obligation on Internet Service Providers (termed IPAP's under the Act) 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/or an order to suspend the internet account holders 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 accountable for the illegal file sharing engaged in by their employees and others who use their internet.

Copyright Act 1994

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 that they hold a copyright in. They also have the exclusive right to issue copies of the work to the public and also to play, perform or show the work in public or communicate the work to the public. These are defined under the Act as "restricted acts". A

Illegal File Sharing

Our guide for Employers and Managers

copyrighted work is infringed if any person, other than the copyright owner or licence holder, does any of these restricted acts. References in the Act to the doing of a restricted act include acts in relation to whole or part of the work and includes directly and indirectly doing restricted acts.

Copyright Infringing File Sharing Regime

Definitions

The Copyright (Infringing File Sharing) Amendment Act 2011 provides a number of definitions which are central to understanding the impact of the Act.

Account Holder in relation to an IPAP, means a person who has an account with the IPAP

Detection Notice means a detection notice issued by an IPAP to an account holder in respect of an alleged infringement against a rights owner

Enforcement Notice means an enforcement notice issued by an IPAP to an account holder in respect of at least 3 alleged infringements against a rights owner

File sharing is defined as circumstances where material that is uploaded via, or downloaded from, the internet where the material is shared through an application or network with other users.

Infringement means an incident of file sharing that involves the infringement of copyright in a work by the person engaging in file sharing.

Infringement Notice means a detection notice, a warning notice, or an 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

The Act refers to **IPAP (internet protocol address providers)** rather than internet service providers to ensure that universities, libraries and businesses that provide internet are excluded and only internet service providers in the traditional sense are included for the purpose of the Act.

IP address means internet protocol address. The IP address is a number that is assigned to internet account holders by their internet service provider.

On-notice period is defined as 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.

A **Quarantine period** is 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 expires and any preceding detection or warning notices also expire.

Warning Notice means a warning notice issued by an IPAP to an account holder in respect of at least 2 alleged infringements against a rights owner

Illegal File Sharing

Our guide for Employers and Managers

Overview

The owner of the copyright will provide the IPAP with the IP address of the user who is alleged to be participating in infringing file sharing of their copyrighted work. Once the information is received from the copyright owner, the IPAP must match the IP address with the account holder who was allotted that IP address when the alleged infringement occurred. The IPAP must then send the account holder an infringement notice within seven days of receiving the information. Where there are multiple instances of infringing, the infringement notice that is sent to the account holder must identify the infringement that triggers the notice. The infringement that triggers the notice in the instance of multiple infringements will be the earliest recorded infringement.

The notice that the account holder receives will vary depending on whether the alleged infringement is the account holders first, second or third alleged infringement.

Notices

From the date of the alleged infringement, the copyright owner has 21 days to send the IPAP the IP address of the alleged infringer. Once received, the IPAP then has 7 days to send out the appropriate infringement notice to the internet account holder.

The notices will be sent via whatever means the IPAP uses to communicate with the account holder for billing purposes unless it is otherwise agreed in writing to use a different method.

The **first** notice that the IPAP will send when it received the first allegation of infringement is the “**detection notice.**” The detection notice remains valid for 9 month or until the expiry of an enforcement notice. The detection notice will:

- identify the rights owner; and
- identify the alleged infringement that has triggered the issue of the notice; and
- identify the date of that alleged infringement; and
- state the date of the detection notice; and
- explain the consequences to the account holder if further infringing occurs; and
- explain how the account holder may challenge the notice; and
- comply with any other requirements that may be prescribed in regulations

The **second** notice that the IPAP will send is the “**warning notice.**” This notice is sent when the IPAP receives an allegation of further infringing however the infringing must occur after the on-notice period and before the expiry of the detection notice. The warning notice expires 9 months after the date of the detection notice or when the following enforcement notice expires. The warning notice will:

- identify the rights owner; and
- identify the infringement that has triggered the issue of the warning notice; and
- identify the date of that alleged infringement; and
- identify the most recent detection notice issued to the account holder in relation to the rights owner (the preceding detection notice); and
- identify any other alleged infringements by the account holder against that rights owner that have occurred since the date of the preceding detection notice; and

Illegal File Sharing

Our guide for Employers and Managers

- state the date of the warning notice; and
- explain the consequences to the account holder if further infringing occurs; and
- explain how the account holder may challenge the notice; and
- comply with any other requirements that may be prescribed in regulations

After the first and second notice there is a 28 day ‘on notice’ period during which any further incidents of infringement will be recorded but will not result in another infringement notice.

The **third** and final notice that an IPAP will send before a copyright owner can bring an action against an infringer is the “**enforcement notice.**” This notice is sent when the IPAP receives an allegation of further infringing however the infringing 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 and once the enforcement notice has expired the preceding detection and warning notices also expire. Once an enforcement notice is sent to an account holder, the IPAP also sends a copy of the notification to the copyright owner. The enforcement notice will:

- identify the rights owner; and
- identify the infringement that has triggered the issue of the enforcement notice; and
- identify the date of that alleged infringement; and
- identify the most recent warning notice issued to the account holder in relation to the rights owner, and the preceding detection notice; and
- identify any other alleged infringements against the rights owner that have occurred since the date of the preceding detection notice; and
- state the date of the enforcement notice; and
- explain that enforcement action may now be taken against the account holder; and
- 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; and
- explain how the account holder may challenge the notice; and
- 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 he or she was the person who actually downloaded or uploaded the infringing file. The account holder will get infringement notices and be fined by the Copyright Tribunal.

Exception

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. Additionally, if the

Illegal File Sharing

Our guide for Employers and Managers

alleged infringement occurred during a quarantine period, the IPAP is not obliged to match the IP address with the account holder.

Where 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. Therefore there is a 28 day on-notice period between the date that the detection or warning notice is sent and the date that the next notice can be sent.

Challenging an infringement notice

An internet account holder that receives an infringement notice has 14 days from the date of the notice to challenge the validity of the notice. The challenge will be 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 by the copyright owner or deemed to be accepted, that notice is cancelled and treated as if it was not sent. However, any preceding notices may remain valid.

Impact on Employers

Businesses should inform those using their internet and explain 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, should an allegation of file sharing infringement by an employee arise. For more information about Discipline please refer to our **A-Z guide on Discipline**.

Copyright owners

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 what the implications are if an employer and / or their employee's engage in file sharing. There are two types of works that employers may encounter: unauthorised copies, and works that the employer, company or employee are authorised to hold a copy of.

Authorised Copies:

Employers should make sure that they have the authority to retain any copyrighted material that has been downloaded on work computers from the internet.

Additionally, employers should ensure that any material that is uploaded onto the internet is done so with the authority of the copyright owner. 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.

Illegal File Sharing

Our guide for Employers and Managers

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 are able to identify who the infringer was, on which computer and how it happened so further infringement can be avoided. Clear guidelines should be developed to reduce your risk of infringing a copyright.

Unauthorised copies:

It is important that employer's understand that any uploading or downloading of unauthorised copies of copyrighted material on the workplace internet may result in the internet account holder (be it the employer or business) receiving a warning. There are some preventative measures that employers could consider using. It is possible to develop a policy that makes any downloading that is not work related serious misconduct.

Contractors and guests:

Employers should be aware that they may be held liable for any infringing file sharing on their internet network. As such, this will include infringements by contractors or other persons who are allowed to access your internet service.

It is important that employers consider how their internet is used and by whom. With this in mind, employers should then consider what preventative measures are required to limit the risk if infringing file sharing occurring on the workplace internet network.

Preventative measures:

There are options available to employers to reduce the risk of infringing file sharing. Some options might be:

- Using Proxy Servers or filtering methods to reduce access to web sites that might allow downloading of copyrighted materials/music/video or software.
- Remove 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.
- Providing notices on work computers advising that internet access is subject to company rules and/or monitoring.
- Make sure your virus protection is up to date
- Password protect your wireless internet so that only authorised users can access the internet

In the absence of an internal IT team, employers might consider engaging an IT contractor to manage their preventative measures.

To discuss preventative measures in more detail, employers should contact an IT specialist and their internet service provider.

Illegal File Sharing

Our guide for Employers and Managers

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 does have a right to prescribe levels or standards of conduct in respect of people, the workplace, and the tools in the workplace. This includes monitoring employee's activity on your computer and internet network to prevent against illegal file sharing. For more information about privacy please refer to the **A-Z Guides on Privacy**.

Best Practice

Employers are encouraged to ensure that their computer and internet usage policy encompasses prohibiting illegal downloading. The policy should include details surrounding what amounts to prohibited use of the company's computers and internet network and how usage will be monitored. The policy should provide a guideline of the investigatory processes and disciplinary processes your organisation has adopted. A clear indication should be given of the consequences of breach of the policy and this should be enforced consistently. For more information about creating and enforcing an internet and computer usage policy, please refer to the **A-Z Guides 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 employee's internet usage. Employers should also consider educating staff as to what amounts to illegal downloading and how to prevent the distribution of copyrighted materials.

It is important that employers monitor their emails as this is 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, employers should contact their IPAP to discuss delivering the notices through an alternative means

Business Central has ER Consultants who would be happy to assist you to draft a computer and internet usage policy. Please contact the Adviceline to be referred to a Consultant.

You can contact one of our employer advisors for telephone advice and assistance: **0800 800 362**; or email the Business Central AdviceLine at advice@businesscentral.org.nz

Illegal File Sharing

Our guide for Employers and Managers

Remember:

- ▶ Always call AdviceLine to check you have the latest guide (refer to the publication date below).
- ▶ Never hesitate to ask AdviceLine for help in interpreting and applying this guide to your fact situation.
- ▶ Use our AdviceLine employment advisors as a sounding board to test your views.
- ▶ Get one of our consultants to draft an agreement template or policy that's tailor-made for your business.
- ▶ Visit our website www.businesscentral.org.nz regularly.
- ▶ Attend our member briefings (held every 4 months) to keep up to date with all changes.
- ▶ Send your staff to Business Central Learning courses and conferences designed for those who manage employees.

© Business Central Inc.

[Reviewed: January 2021]