Australia's Online Service Provider Safe Harbours - Guide for Libraries and Archives

Background

The safe harbour provisions of the Australian *Copyright Act 1968* (ss116AA-116AJ) grant online service providers protection when their facilities are used to infringe copyright. Under the provisions, service providers do not have to pay financial damages for infringements undertaken by others on their systems as long as they take certain steps designed to limit the impact on copyright owners.

The *Copyright Amendment (Service Providers) Act 2018*, which comes into effect on Friday 29 December 2018, extends these safe harbours - which originally only applied to commercial ISPs - to include cultural, educational and disability groups where they provide certain online services to the public. In order to obtain the extra protections, these organisations must comply with a series of requirements prescribed by the legislation.

Importantly – compliance with the safe harbours is entirely voluntary, and **institutions are not legally required to comply with the steps below**. If you do choose to comply with the safe harbour requirements, you will receive additional legal protections that lower your financial risk in relation to your activities as a service provider. However, not complying with the safe harbours does not make you liable for infringing activities by your clients – you will merely be in the same legal position you were prior to the legislative changes.

This Guide

This Guide provides a description of the Australian safe harbour scheme, the services it applies to, and the requirements that institutions must comply with to access the safe harbours for their services. It is divided into 4 major sections:

1. Services to which the safe harbours apply
2. Checklist A: Compliance steps for all institutions
3. Checklist B: Notice and takedown process for institutions providing hosting services
4. Copyright Safe Harbour Quick Checklist

Both Checklists also include compliance flowcharts.

The information in this guide is general in nature and **it is not legal advice**. For specific situations you may need to seek advice from a lawyer. The guide also deals exclusively with compliance with the online service provider safe harbours. Other copyright or non-copyright issues may arise from the provision of online services for clients on which you should obtain separate advice.

Services to which the safe harbours apply

The services to which the safe harbours apply are divided into the following categories:

A. Providing facilities to access the internet - eg public access computers or wifi;

B. Automatic caching - eg as part of providing computers or servers that are used to search online;

C. Storing or hosting materials for clients - eg a repository or website to which clients can upload materials – note that this does not apply to materials that have been selected or curated by the institution, but only those uploaded directly by users without changes or moderation; and

D. Linking to third party materials - eg running a custom search engine or providing a directory of resources on external websites.

While most libraries and archives provide services that fall within categories A, B and D, only a small number are likely to provide services in categories C. For example, the National Library of Australia's new online legal deposit system would likely fall within category C as deposits are made public immediately with no moderation by NLA staff. So would community engagement projects that encourage the public to contribute content to an online space or allow those working at a Digital Hub to upload their content to a website without approval or moderation. However, digitised collection archives like Pandora or Trove that have been curated by institutional staff would not.

The checklists below separate out the steps that institutions providing services in categories A, B and D (assumed to be all institutions) should take if they wish to access the safe harbours from those that only apply to the smaller group of institutions providing category C hosting services.

Compliance requirements for services

In addition to falling within the above categories, the services themselves also need to meet certain requirements to fall within the safe harbours. These requirements vary depending on the service being provided. They are generally already standard in the sector, so it is expected that most institutions' services will already be in compliance with these requirements. However, it is worth checking that your relevant services do have the features below. If they do not, the safe harbour will not apply to those services.

1. **For internet access and caching services - you must not substantially modify the material being transmitted or cached**
    - The safe harbours only apply to services that provide public access to the internet or caching if you do not make "substantive modifications" to the material being transmitted or cached.
    - If you are actively modifying or adapting content that passes through your systems you may not be able to use the safe harbour protections for those services.
    - This does not prevent you from making technical modifications as part of the communication process. Technical modifications taken without human intervention would not normally be considered "substantial".
    - In practice, it is expected that most institutional systems will already be set up to comply with these requirements.

2. **For hosting and linking services - they must be free (ie you must not receive a financial benefit that is directly attributable to infringing activities)**
    - In practice, it is not expected that many institutions in these sectors would be charging for or otherwise receiving a financial benefit from providing hosting or linking services to the public.
    - However, if your institution does, for example, charge for online hosting for clients, you may not be able to use the safe harbour protections for those services, even if the charge is only cost recovery.
    - This limit **does not apply to category A or B services** ie you can charge for public internet access or wifi, or for services that use your cache, and still receive safe harbour protection for these services
3. **For hosting services - you must not choose the material being hosted**
    - The safe harbours only apply to materials uploaded to hosting services "at the direction of the user." This means that the safe harbours do not apply to material that has been digitised and made available online by your staff even if that material is created by third parties and has not been modified.
    - It also means it won't apply to user generated content projects if the material is selected or approved by library staff before it is posted online. It will, however, apply to projects where users upload material directly themselves.
    - This does not prevent you from making technical modifications as part of the upload process, as long as the upload was still at the request of a client.
4. **For caching services - you must respect technical restrictions**
    - This essentially requires you to set up your system to respect any technical restrictions (eg password protection) when you are caching material.
    - In practice, it is expected that most institutions systems will already be set up to comply with these restrictions.

What if my services aren't covered by the safe harbour?

Remember, the safe harbours are voluntary, so you do not need to change your services to comply. For example, if you are providing internet hosting services for which you are charging a fee, you can continue to do so. But be aware that you will not have safe harbour protection for that service. This does not mean you will be held liable for any infringements clients undertake on the service, but it does mean that you will be at greater financial risk should this happen.

Even for services that do not fall within the safe harbours, will usually still a good idea for you to have policies and procedures in place covering the kinds of issues addressed by the safe harbours eg for takedown of allegedly infringing material or dealing with repeat infringers. This may help to reduce your legal risk for these services, even in the absence of safe harbour protection. These policies could draw on the safe harbour system set out above, but do not have to follow its strict requirements. For example, you may require a "higher bar" in terms of evidence and review before taking down material that has been uploaded by your staff rather than a client.

Checklist A: Compliance steps for all institutions

Institutions that provide facilities to access the internet (eg public access computers), undertake automatic caching, or provide custom search or linking services should follow the steps below if they wish to access the safe harbours.

1. **Provide the title of and contact details for a designated person to receive copyright notices on your website**

   - The position title of the designated representative must be included in the website notice, along with sufficient information to allow them to be contacted. This could be in the form of an email address or via an automatic form.
   - The legislation allows institutions to provide the details on either their own website or on that of their administering body (eg the local education department where the school does not maintain their own website). If in doubt as to which website should have the contact details, add them to both.

For example: an institution has a link to a copyright page in the footer of its website. On that page it sets out its copyright policy and states that the institution's Copyright Officer is the designated contact for copyright inquiries and takedown requests. It provides an online form to allow people to send requests to the Copyright Officer.

2. **Have a policy for termination, in appropriate circumstances, of the accounts of repeat infringers**

   - This requires you to have a policy for the termination of accounts of people who have repeatedly infringed copyright using your systems.
   - This policy can be internal, but should be written and recorded as evidence of its existence, and it must be "reasonably implemented" ie there must not be evidence of you ignoring repeat infringers.
   - There is no definition of "infringer" in the legislation – this could in theory be taken as only applying where a user has been found to have infringed copyright by a court of law. However, best practice for the libraries and archives sector would be for it to apply once you become aware of credible allegations of repeated infringing behaviour by a user (eg due to multiple takedown notices or through your own observations).

For example: an institution hosts a community engagement project in which users are encouraged to upload digital artworks to a web platform. Over a 12 month period it receives three credible notices that a particular user's work contains infringing materials and takes the materials down as a result. After the third notice it terminates the user's account on the service.

3. **Remove material from your cache if it has been removed from the original site for being infringing**

- This provision relates to material that might be stored in a cache on your public computers or servers. If that material has been taken down from its original website because it is infringing, you are required to remove it from your public computer caches. This is to stop the material from being available via the web services of the institution after it is no longer available at the originating site.
- In practice, these notices are unlikely to be received often. However, institutions should be aware that if they do receive such a notice, they should comply.
- The notice should be in the form prescribed by the legislation. However, if it is not in that form but still contains the relevant information, it is good practice to accept it. If it does not provide the relevant information, you may wish to respond with a link to the form for them to fill out.
- As these notices are sometimes sent in error or fraudulently, it is good practice to check the veracity of the notice before removing the material from the cache ie to check that the material has actually been removed from the originating website.
- Once you have determined the cached material should be removed, the removal must be "expeditious." This is not legally defined, but the aim should be to remove the material as soon as possible, usually within three working days.

For example: a copyright owner finds their material has been uploaded to the website http://example.com.au without their permission and has the material taken down. They then send notices to a library where they believe the material may have been accessed informing them of the takedown and asking them to remove the material from their caches. In response, the library deletes all copies of http://example.com.au from their cache.

4. **Remove any links you provide on your system that point to third party material that is infringing**

- This provision relates to links that you provide on your public access systems eg as part of a reference page on your website or a custom search engine.
- If you become aware - either through notification by the copyright owner or through your staff activities - that a link points to material that is infringing, you are required to remove the link from your services.
- The notice:
    - must be from the owner or exclusive licensee of the material, or their agent;
    - must state that the owner/licensee/agent believes, on reasonable grounds, that the material to which it links is infringing; and
    - should be in the form prescribed by the legislation. However, if it is not in that form but still contains the relevant information, it is good practice to accept it. If it does not provide the relevant information, you may wish to respond with a link to the form for them to fill out.

- As these notices are sometimes sent in error or fraudulently, it is good practice to check the veracity of the notice before removing the material ie check that the person sending it appears to be the copyright owner and that the material is what they claim it is (eg not just another work with a similar title).

For example: an institution provides a list on its website of places to get openly-licensed material that can be legally reused, which includes a link to a website http://freemusic.net. This website is taken to court and found to be providing infringing content. When a library staff member sees a news story about the court case they remove the link from the list.

5. Comply with any relevant industry codes

- This provision only applies to codes relating to:
    - accommodating and not interfering with technical measures used to protect and identify copyright material; or
    - updating cached material.
- At the time of writing this checklist, no qualified codes exist or are planned.
- If in future libraries and archives enter into codes on these subjects with rights holders, it will be a requirement to comply with them to access the safe harbour.

Copyright Safe Harbour Flowchart for All Institutions

Do you provide public access computers or wifi, or public access services that use caching?

NO

Do you provide services that link to external websites eg a custom search engine or reference list?

Yes

Are these services automatic ie the material is not modified by your staff?

NO

Yes

Are these services free?

Yes

No

Yes

No

The copyright safe harbours cover your services. You should consider taking the compliance steps below to access additional legal protections.

You do not provide services covered by the copyright safe harbours. You do not need to take any action.

Next

Compliance Steps

1. Provide the title of and contact details for a designated person to receive copyright notices on your website

Next

2. Have a policy for termination, in appropriate circumstances, of the accounts of repeat infringers

Next

3. Remove material from your cache if it has been removed from the original site for being infringing - as soon as practicable after receiving a takedown notice from the copyright owner/licensee (usually within 3 working days)

Next

4. Remove any links from your system that point to infringing material - as soon as practicable after receiving a takedown notice from the copyright owner/licensee (usually within 3 working days)

Next

5. Comply with any relevant industry codes (none currently exist)

Checklist B: Notice and takedown process for institutions providing hosting services

In addition to the above steps for all institutions, institutions providing a service that hosts material at the direction of third parties (ie a hosting service) will need to comply with the following notice and takedown procedure for any allegedly infringing material on their system if they want to access the safe harbours for those services. It is similar to the notice and takedown procedures most institutions will already have in place, but requires certain forms and processes.

A hosting service would, for instance include a site where you allow users to upload material they have created as part of a competition, community outreach or open access repository. It will not include any service where your institution is responsible for selecting or uploading the material (eg a curated online collection) or where you select content before it is published (eg a user generated content platform where material is moderated before it is publicly viewable).

If you charge for the hosting service or otherwise receive a financial benefit directly attributable to it, it will not be covered by the safe harbour.

Notice and takedown procedure

6. **Remove material that has been uploaded at the direction of a client if:**

    a) **you receive a credible takedown notice alleging that it is infringing; OR**

    - The notice must be from the owner or exclusive licensee of the material, or their agent.
    - The notice should be in the form prescribed by the legislation. There are different forms if the material has been found to be infringing by a court, or if the copyright owner/licensee just has a good faith belief that it is infringing.
    - If the notice is not in the appropriate form but still contains the relevant information, it is good practice to accept it. If it does not provide the relevant information, you should respond with a link to the form for them to fill out.
    - As these notices are sometimes sent in error or fraudulently, it is good practice to check the veracity of the notice before removing the material ie check that the person sending it appears to be the copyright owner or their agent, and that the material is what they claim it is (eg not just another work with a similar title). This should be done expeditiously.

    b) **you become aware that it is infringing**

    - You are not required to “hunt down” infringing materials on your system, or to otherwise monitor communications. However, if your staff does discover material they suspect to be infringing on your system in the course of their work, it should be taken down.

    The removal must be “expeditious.” This is not legally defined, but the aim should be to remove the material as soon as possible, usually within 3 working days.

7. **Notify the user who uploaded the material to your system that it has been taken down**
    - As part of doing this, you must send them a copy of the notice of claimed infringement, so they have the details.
    - You should also tell them that they have 3 months to issue a counter-notice disputing the claim.
    - The counter-notice should be in the form prescribed by the legislation. There are different counter-notice forms if the material was taken down in response to a notice by the copyright owner/licensee, or taken down on the initiative of the institution.

8. **If you receive a counter-notice, send it to the copyright owner or their agent**
    - In doing so you should inform the owner/agent that they have 10 working days to seek a court order restraining the activity, or else the material will be restored.

9. **If the copyright owner notifies you they are taking court action within 10 working days, keep the material down. If they do not, or if the action was unsuccessful, restore the material.**

For example: an institution is running a competition in which it encourages users to upload videos using its public domain materials to a special website it has set up. It receives an email from a record label claiming to be the copyright owner of music used in one of these videos, with a notice and takedown form attached.

The institution checks that the song is the one the record label identifies, and that the record label is the original publisher of the material, and then disables access to the material. It sends the notice on to the original uploader of the material, notifying them that the material has been removed. When it does not get a counter-notice from the original uploader within 3 months, it leaves the material down.

Copyright Safe Harbour Flowchart for Hosting Institutions

Do you host other people's materials on your servers (eg as part of a user generated content project, or e-legal deposit)?

Yes

Do you allow clients or users to upload material directly to this service, without your approval or selection?

Yes

Is this service free?

Yes

The copyright safe harbours cover your hosting service. You should follow the takedown process below in relation to any potentially infringing content uploaded by third parties.

Next

Have you received a takedown notice from a copyright owner/licensee alleging that material on your hosting service infringes copyright?

Yes

Is the notice credible? eg Is the material correctly identified? Does the person sending it appear to be the copyright owner/licensee or their agent?

Yes

No

No

No

The copyright safe harbours do not cover your hosting service. You can determine your own takedown process.

OR

Have you found material on your hosting service you believe infringes copyright?

Yes

Takedown Process

1. Remove the material from your service as soon as practicable, usually within 3 working days.

Next

2. Notify the person who uploaded the material that it has been removed, and inform them that they have 3 months to issue a counter-notice challenging the claim that the material is infringing. Include a copy of any takedown notice you received from the copyright owner/licensee for information.

Next

3. If you receive a counternotice, send it to the copyright owner/licensee and inform them they have 10 days to commence legal action.

Next

4. If the copyright owner/licensee does not inform you they have commenced legal action in 10 days, or if the action is unsuccessful, restore the material.

Copyright Safe Harbour Quick Checklist

What services are covered?

A. **Providing facilities to access the internet** - eg public access computers or wifi - where you do not substantially modify the content being transmitted

B. **Automatic caching** - eg as part of providing computers or servers that are used to search online - where you do not substantially modify the content being cached and where you respect any technical restrictions such as password protection on the material being cached.

C. **Hosting materials for clients** - eg by providing a repository or website where clients can upload materials – where the materials have not been selected or curated by you or your staff,[1] and where you do not charge or otherwise receive a financial benefit from the service.

D. **Linking to third party materials** - eg running a search engine or providing a directory of resources on other websites - where you do not charge or otherwise receive a financial benefit from the service.

Compliance steps for all institutions

These steps should be followed by institutions that provide facilities to access the internet (eg public access computers or wifi), undertake automatic caching, or provide custom search engines or linking services.

1. Provide the title of and contact details for a designated person to receive copyright notices on your website.
2. Have a policy for termination, in appropriate circumstances, of the accounts of repeat infringers.
3. Remove material from your cache if it has been removed from the original site for being infringing – as soon as practicable after receiving a takedown notice from the copyright owner/licensee, usually within 3 working days.
4. Remove any links from your system that point to infringing material – as soon as practicable after receiving a takedown notice from the copyright owner/licensee, usually within 3 working days.
5. Comply with any relevant industry codes if they exist (none currently do).

Notice and takedown system for hosting services

In addition to the above, institutions providing hosting services should follow the below notice and takedown procedure for any allegedly infringing material uploaded by others to their system.

6. Remove material uploaded by third parties to your system as soon as practicable (usually within 3 working days) after you:
   a) receive a credible takedown notice from the copyright owner/licensee alleging that it is infringing; or
   b) become aware that it is infringing.
7. Notify the user who uploaded the material to your system that it has been taken down, and they have 3 months to issue a counter-notice challenging the claim of infringement.
8. If you receive a counter-notice, send it to the copyright owner/licensee, informing them they have 10 working days to commence legal action.
9. If the copyright owner/licensee does not notify you within 10 working days that they have commenced legal action, or if the action is unsuccessful, restore the material.

[1] Note that this only applies to services where materials have been chosen and uploaded by clients – if your institution is responsible for selecting or uploading the material (eg a curated online collection) or actively moderates content before it is uploaded (eg a user generated platform where material is selected by staff) the safe harbour does not apply to that service.