

## ***Rights metadata use cases for preservation: National Library of Australia***

(Contact: Gerard Clifton, [gclifton@nla.gov.au](mailto:gclifton@nla.gov.au))

We have a range of materials for which we take preservation responsibility, including both published and unpublished materials. Some rights differences will exist due to this distinction, but we expect that the rights we will need to obtain for preservation purposes will be similar across all the material types.

### **Types of materials**

- Unpublished manuscript materials in digital form (letters, email, documents, images)
- Unpublished sound recordings
- Digitised images, manuscripts, sheet music, publications
- Published physical format materials – monographs and serials, maps
- Online materials – electronic journals, Web sites, online documents

### **Stakeholders**

- Depositor of the material (either through voluntary deposit or acquired under legislation) (May or may not be the original rights holder)
- The Library, including collection management and preservation staff
- Owner of the file format or third party software used to support or create the material, if applicable.
- End users

### **Assumptions**

We would keep at least retain a copy of the original files as received or created (Bit level preservation), (and would do so even if further preservation action was involved) but would also aim to provide access to as accurate a representation of the original as possible in the future (Optimal level preservation).

Depending on the type of material, this may involve

- normalization or migration of the material (for images, textual documents, data sets, databases etc.),
- use of access tools (e.g. viewers) to interpret the original (or normalised) material for new environments,
- emulation of original environments to access the material (e.g. multimedia, software).

This assumes we have permissions:

- *to make preservation copies of original materials*  
[Duplicate - pre-ingest or ingest]
- *to make additional access copies* (to protect the preservation copies from use)  
[Duplicate - pre-ingest or ingest]
- *to take action on the materials for continued access*

This would involve, at a bit preservation level:

- Multiple backups and copying to fresh media [Duplicate]
- Integrity checks, etc.

This would also involve, for optimal preservation:

- modification of the original material (e.g. replacement of line breaks, fixing of links or internal scripts to work within the repository delivery environment)  
[Modify – pre-ingest, preservation management]
- or may require transformation (normalisation, migration), creation of derivatives or reverse engineering of materials for continued access in a new environment.  
[Modify - preservation management].
- *to simultaneously retain more than one copy of transformed materials.*  
We may want to retain previous generations of materials for 'back-tracking' if the present preservation pathway comes to a dead end.  
[Duplicate, Backup/Restore - storage, data management]
- *to retain and (re)use copies of required supporting software* (including operating systems) for access to materials via approaches such as emulation.  
[Duplicate, Install, Distribute]
- *to provide access to materials via new distribution channels that may evolve.*  
This is primarily an access issue, but may have an effect on limiting what preservation actions may be taken.  
[Modify , Distribute]
- *to transfer all these rights to another custodian*, should the materials need to be transferred to another repository.  
[Distribute, Transfer]
- *to withdraw or delete the item from the repository* [Withdraw, Delete]

An additional issue is that a depositor may not have the right to confer all these rights. For example, document formats or multimedia engines used within publications may be proprietary, and granting the right to reverse-engineer the publication may not rest with the creator or depositor, but with the software developer of the tools used to create the publication.

Other events that would occur in the repository processes would include virus checking, integrity and authenticity checking, but it is not clear that permissions would be required to undertake these actions.

### **Constraints on the permissions**

No specific scenarios, but we can imagine that these aspects may be involved:

*Time* – likely to have effects on validity of other rights constraints (e.g. expiration of copyright, patents)

*Purpose* – some actions may be allowed for particular purposes, but not for others (e.g. duplication for archival purposes, but not for distribution; duplication for non-commercial purposes)

*Number* - may limit the number of copies, versions, instances that may be retained (or accessed) simultaneously.

*Attribution* – use or actions (e.g. transformations) may be allowed if correct attributions are given (e.g.. Open Source software licensing, inclusion of copyright notices)

*Format* or *Quality* - may constrain what transformations may be undertaken (e.g. streaming formats may forbid capture or transformation to other formats, or a depositor may limit the manner in which their work may be represented).

Other constraints, such as *Distribution scope* (e.g. stand-alone, web accessible, single-user, not available for loan) are related to access conditions rather than preservation actions, but may affect choice of preservation pathways (e.g. do we need to facilitate viewing this in a Web environment if we are constrained to stand-alone access?) or the number of copies that may be retained.

There may also be facilitators rather than constraints that may be usefully explicitly stated (e.g. “may be freely distributed”, “for all purposes”, etc.).