

# Disposal (CPP-017)

<b>CPP-Identifier</b>	CPP-017
<b>CPP-Label</b>	Disposal
<b>Author</b>	Mikko Laukkanen, Juha Lehtonen
<b>Contributors</b>	Kris Dekeyser, Johan Kylander
<b>Evaluators</b>	Matthew Addis, Felix Burger, Maria Benauer
<b>Date of edition completed</b>	29.08.2025
<b>Change history</b>	<b>Comments</b>
Version 1.0 - 29.08.2025	Milestone version

# 1. Description of the CPP

The TDA enables the managed disposal of *Information Packages* and permits the retention and maintenance of *Metadata* even when the content of the *Information Package* has been removed from the TDA.

## Inputs and outputs

Input(s)	
Data	<i>Information objects</i>
Metadata	<i>Rights metadata</i>
	<i>Technical metadata</i>
	<i>Descriptive metadata</i>
Documentation / guidance	Appraisal reports
	Quality reports
	Retention Policy
Organisational inputs	Policies
	Legal aspects (e.g. licenses)
Output(s)	
Metadata	<i>Provenance metadata</i>
	Tombstone metadata
Documentation / guidance	Audit trails
	Possible certificates/records of disposal (especially in the case of sensitive or confidential data)

## Definition and scope

Disposal refers to the process of removing or decommissioning *Information objects* from a TDA when its preservation is no longer needed or possible, or the *Object* has fulfilled its short-term preservation requirements. The latter requires appraisal and scheduling, where institutions establish clear policies defining how long different types of *Objects* should be preserved. Disposal is usually triggered on *AIP* level.

Disposal can be triggered by the following reasons:

- The TDA no longer has a legal basis to retain data (e.g. there is no consent);

- The TDA has been requested to remove data (e.g. there is a legitimate take down request);
- The TDA has transferred data to another TDA and no longer needs to retain the data;
- The data is no longer usable by the designated community (e.g. because it has been corrupted or damaged and is beyond repair, or because quality assessment shows that it is no longer usable);
- The data is no longer being used by the designated community, there is no expectation of future use, and organisation policy requires it to be disposed of (e.g. to reduce operational costs);
- The retention period for data has expired and the data should be disposed of (e.g. to ensure regulatory or legislative compliance);
- The TDA has alternative versions of the data that allow the original to be disposed of (e.g. as a result of normalisation or migration, or because a depositor has provided a superior version);
- The funding bodies that support the TDA no longer require or fund retention of the data (e.g. because the data no longer has funding body requirements for it to be accessible);
- The TDA elects to dispose of data (e.g. to help ensure its long-term sustainability in economic or ecological terms).

The TDA must have a disposal policy, that in addition to the disposal of *Objects* or (derivative) *Files* includes related *Technical* and *Descriptive metadata*. This is especially important when the related *Metadata* contains sensitive or confidential information. The policy may state that all or most of the *Metadata* is retained, disposed, or something in between. However, at minimum, TDA must create and retain provenance *Metadata* about the disposal and provide (e.g. some “tombstone metadata” for keeping the PIDs resolvable).

The TDA must also consider the technical aspects of disposal, such as secure deletion methods that prevent data recovery, and the potential impact on related *Objects* that may reference the disposed items.

As the *Objects* can be copied and distributed across multiple storage systems and different storage media within a TDA, the complete physical removal of all copies might be complex and needs a timeframe. For instance, whereas a *File* is quick and easy to remove from a hard drive, it may be practically impossible to remove it from a magnetic tape. Thus, the actual disposal of copies of *Files* on tapes may occur only at the time when the tape is refreshed (i.e. the disposed *File* is then not included on the new tape). Therefore, the first step to do could be a “logical disposal” (i.e. preventing access to the *Object*, which gives time for the TDA to dispose of the physical copies). Sometimes this is referred to as “Deaccessioning” where *Objects* are removed from the collections that an organisation holds before the *Objects* are physically disposed of. The storage management information must be updated accordingly.

Disposal decisions must be made carefully, as recovering disposed *Objects* may be impossible after physical deletion has been performed. Thus, effective disposal requires clear policies, robust documentation, secure technical procedures, and ongoing monitoring. The disposal process must produce audit trails and other relevant documentation about the disposal. An organisation may choose to implement additional safeguards as part of the disposal process depending on the type of data they hold. For example, data may be moved to a ‘trash bin’ for a period of time before permanent deletion takes place, which can be used to provide a short-term recovery window to guard against unwanted deletion (accidental or deliberate). Request, review or approval processes may also be employed. For example to prevent permanent deletion of an *Object* without explicit and documented approval from a requisite number of staff members who are authorised to approve disposal.

## Process description

### Trigger event(s)

Trigger event	CPP-identifier
<i>Information packages</i> or <i>Files</i> are identified as corrupted and not recoverable. Data corruption management triggers the disposal.	CPP-004 (Data Corruption Management)
Changes to community needs	CPP-018 (Community Watch)
The data quality assessment tasks may discover intolerably low-quality issues in a digital <i>Object</i> and provide a trigger for disposal	CPP-019 (Data quality assessment)
Changes in legislature, rights, regulations, licenses, standards and alike	CPP-020 (Rights management)
Detected risks	CPP-023 (Risk definition and extraction)
The file repair process may end up with a situation where the <i>File</i> cannot be repaired. In such cases, disposal is required by the file repair process.	CPP-027 (File Repair)

### Step-by-step description

No	Supplier	Input	Steps	Output	Customer
1a	CPP-004 (Data Corruption Management)	Quality reports	TDA finds out, from management events or other triggering events, that an <i>AIP</i> or <i>File</i> is corrupted	Storage management information (list of affected <i>AIPs</i> , <i>Files</i> )	

	CPP-027 (File Repair)		and is not recoverable. The TDA decides to dispose of it.	Disposal request	
1b	CPP-018 (Community Watch)	Changes to the needs of the designated community	The designated community no longer has a need for the data, it is demonstrably not making any use of the data, and there is no expectation that it will make any future use of the data. Therefore, the TDA decides to dispose of the data.	Storage management information (list of affected <i>AIPs</i> , <i>Files</i> )	
				Disposal request	
1c	CPP-019 (Data quality assessment)	Quality reports	The quality of the data no longer meets the minimum requirements of the designated community or the data is available in an alternative and higher quality version or format. Therefore, the TDA decides to dispose of the data.	Storage management information (list of affected <i>AIPs</i> , <i>Files</i> )	
				Disposal request	
1d	CPP-020 (Rights management)	Quality reports	TDA gets a trigger event indicating that an <i>AIP</i> or <i>File</i> needs to be disposed of.	Storage management information (list of affected <i>AIPs</i> , <i>Files</i> )	
		Intellectual property change			
		Risk detection			
	CPP-023 (Risk definition and extraction)			Disposal request	

1e		Appraisal reports	The retention period of the data has been fulfilled according to the appraisal or reappraisal of the data.	<i>Storage management information</i> (list of affected AIPs, Files)	
2		<i>Storage management information</i> (list of affected AIPs, Files)	<p>Creation of a disposal plan for the data in question from the policy. It should address the following issues:</p> <ul style="list-style-type: none"> <li>- Creation of tombstone metadata for PIDs</li> <li>- Defining the retention period between logical disposal and physical disposal</li> <li>- Documenting the disposal request</li> </ul>	Disposal plan	
		Disposal request			
		TDAs policy on disposal			
3		Disposal request	Document the disposal request (such as the reason), the affected AIPs or Files, timestamps	<i>Provenance metadata</i>	
4		Disposal plan	Implement deaccessioning/logical disposal. Prevent access to the <i>Object</i> , its discovery, and exclude it from any external reporting (such as statistical data generation).	<i>Provenance metadata</i>	
		<i>Storage management information</i>			
5		Disposal plan	If identifiers exist: the creation of tombstone metadata.	Tombstone metadata	

6		Disposal plan	Physical disposal of copies from primary random access media, such as hard disk drives. Update <i>storage management information</i> (removal of storage locations).	<i>Storage management information</i>	
				<i>Provenance metadata</i>	
7		Disposal plan	Physical disposal of copies from secondary sequential access media, such as magnetic tapes and off-line copies. Usually done at later stages during (e.g. Refreshment). Update <i>storage management information</i> (removal of storage locations).	<i>Storage management information</i>	
				<i>Provenance metadata</i>	
8		Disposal is complete.	If evidence is required that disposal has been completed, then create a certification of destruction that confirms that all copies of the data have been permanently deleted.	Destruction Certificate	

## Rationale(s)<sup>1</sup> and worst case(s)

Rationale	Impact of inaction or failure of the process
Disposal could be legally mandatory in terms of privacy and retaining only necessary content.	Legal consequences
Not disposing of data in a timely way results in unnecessary and irrelevant content being retained. This could worsen the consequences of cyber attacks (e.g. ransomware of data that should have been disposed of before the attack). Or if the data is compromised then it could result in privacy breaches.	Exploitation of security vulnerabilities, more costly to recover from cyber attacks, data privacy breaches
Retaining data that is no longer needed can impact on data quality and integrity. Removing outdated, duplicated, or corrupted <i>Objects</i> helps maintain the quality and usability of the TDA.	Reduction in data quality and integrity
Removing data reduces the TDA's storage and processing footprint.	Increased costs data storage costs. Increased environmental footprint. Increased time and effort for future preservation activities (e.g. re-appraisal)

## 2. Dependencies and relationships with other CPPs

### Dependencies

CPP-ID	CPP-Title	Relationship description
CPP-005	Identifier Management	Identifiers must be taken care of during disposal
CPP-018	Community Watch	Soft dependency (i.e. may require): Community watch treats Disposal as a customer in cases where, for instance, a collection previously archived within the TDA has been also added to a different TDA and will be preserved there. Required actions downstream must be taken into account within the disposal process (e.g. notifying stakeholders about the changed preservation

<sup>1</sup> Term derived from PREMIS.



		location).
CPP-025	Enabling Access	Disposal prevents access to the <i>Objects</i> . Also, preventing access can be considered as “logical disposal”

## Other relations

Relation	CPP-ID	CPP-Title	Relationship description
Required by	CPP-016	Metadata Ingest and Management	A tombstone consisting of only <i>Metadata</i> - without the actual data - has to be kept as a witness of the data's former presence.
Not to be confused with	CPP-006	AIP Batch Export	Disposal does not export the <i>Objects</i> from TDA.

## 3. Links to frameworks

### Certification

Certification framework	Term used in framework to refer to the CPP	Section
CTS <a href="#">Link</a>	Deletion	R14 The repository applies documented processes to ensure data and <i>Metadata</i> storage and integrity.
Nestor Seal <a href="#">Link</a>	/	/
ISO 16363 <a href="#">Link</a>	Disposal Disposal records	3.3.3. 4.2.3.3.

### Other frameworks and reference documents

Reference Document	Term used in framework to refer to the process	Section
OAIS <a href="#">Link</a>	Deletion	3.3.6
PREMIS <a href="#">Link</a>	Deaccession	Glossary

## 4. Reference implementations

### Publicly available documentation

Institution	Organisation type	Language	Hyperlink
TIB – Leibniz Information Centre for Science and Technology and University Library, Germany	National library	English	<a href="https://knowledge.exlibrisgroup.com/Rosetta/Product_Documentation/Rosetta_Staff_Users_Guide/Data_Managers/005_Delete%2C_Restore%2C_Move%2C_and_Purge_IEs#About_Deleting.2C_Recovering.2C_and_Purging_an_IE">https://knowledge.exlibrisgroup.com/Rosetta/Product_Documentation/Rosetta_Staff_Users_Guide/Data_Managers/005_Delete%2C_Restore%2C_Move%2C_and_Purge_IEs#About_Deleting.2C_Recovering.2C_and_Purging_an_IE</a>
	Non-commercial digital preservation service		
	Research infrastructure		
	Research performing organisation		
Archivematica	Digital preservation system	English	No explicit support for retention management, but there is a request/approve workflow for AIP deletion: <a href="https://www.archivematica.org/en/docs/archivematica-1.17/user-manual/archival-storage/archival-storage/#delete-aip">https://www.archivematica.org/en/docs/archivematica-1.17/user-manual/archival-storage/archival-storage/#delete-aip</a>