Academic Preservation Trust Collection Development Policy

Scope

This Policy applies to all digital content and associated metadata deposited in the APTrust for long-term preservation. This policy does not address decisions on subject matter and content format chosen for deposit, which are solely determined by depositing members.

Objectives

This Policy establishes guidelines about the nature of digital content that may be placed in the APTrust repository.

Document Conventions

- The capitalized key words "MUST," "MUST NOT," "REQUIRED," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" are to be interpreted as described in RFC 2119.
- Terms in *italics* are defined in the **Definitions** section below.

Principles

- 1. Academic Preservation Trust (APTrust) dedicated to the long-term preservation and curation of (archival, cultural heritage, and scholarly) digital content submitted by its partner institutions.
- 2. The aggregate repository is envisioned to collect many forms of content, support administrative access, augment the preservation plans of individual institutions, and provide a firm foundation for exploring future access services.
- 3. APTrust will leverage investments that institutions are making separately and will strive to accelerate the implementation of effective digital preservation solutions for partner institutions.

Policy Statement

Types of Allowed Content

- 1. Content deposited in APTrust MAY be in any computer file format—from image files, motion media, web archives, disk images, etc. There are no restrictions to the item types at this time.
- 2. Deposited content SHOULD be in accord with depositing institution's own policy.
- 3. Deposited content SHOULD be submitted following evolving best practices and APTrust guidelines.
- 4. Metadata describing the manifest (BagIt bag) / file package contents MUST include the following types:
 - a. Institution (controlled vocabulary)
 - b. File type (mime)
 - c. Title open
 - **d.** Bag Name open

- e. Rights/IP (controlled vocabulary APTrust will encourage the use of <u>rightsstatement.org</u> protocols)
- f. PID institutional specific

Restrictions on Content

- 8. Deposited content MUST NOT contain sensitive or personally identifying information unless encrypted.
- 5. Depositors MUST deposit content at their own risk.

Removal of Content

9. Removal of content will take place only at the instruction of the depositing entity or by decision of the APTrust Governing Board if the original depositing entity does not or is unable to provide instructions.

Definitions

Term	Definition		
Bag	 A payload of digital content defined in the Bagit hierarchical file packaging format 		
Personally identifying information (PII)	 Used in information security and privacy laws, PII is information that can be used to identify, contact, or locate a single person, or to identify an individual in context. Precise legal definitions may vary by jurisdiction. 		

Roles and Responsibilities

Role	Responsibilities		
APTrust Advisory	•	Oversees and advises on the development and revision of this policy.	
Committee	•	Monitors policy status and initiates review at the appropriate time	
APTrust Governing	Approves final policy drafts		
Board	•	Requests new policy development from the Advisory Committee	

Related Documents

- Language and ideas were borrowed from the following sources, which were consulted during the drafting of this policy:
 - o <u>Bagit</u> definition from Wikipedia
 - PII definition from Wikipedia

NOTE: Other items may be added to this section without requiring policy revision

Review

Review frequency: No less frequently than two years from adoption or previous review

Version History

Version	Status	Date	Notes
0.1	Draft	7/13/17	BJD draft and shared with Communications Group
0.5	Draft	9/26/17	Shared with Advisory for feedback
0.7	Draft	1/12/18	Advisory Changes incorporated
.8	Draft	2/1/18	Final review by Advisory
1.0	Final	4/2018	Board Approved