Appendix 5: Rubric for Privacy Policy Reviews

PART ONE – The policy itself
This part of the rubric is organized to align with the template for privacy-related library policies.

I. Title.
   • Does it have a title?
   • Is the title meaningful and distinct from other policy titles?

II. Background / Purpose.
   • Why does the policy exist?
   • What are the driving and/or extenuating circumstances that require this particular policy in addition or exception to general Library policy?
   • Is the context provided, such as legal requirement versus professional ethics?

III. Policy points to be addressed
   a. Notice/Awareness
      • How are users and patrons informed of and directed to this policy?
      • How are Library Faculty and staff informed of and directed to this policy?
      • How are changes to the policy vetted and communicated?
      • Are the following points addressed and to what extent?
         o identification of the entity collecting the data; identification of the uses to which the data will be put;
         o identification of any potential recipients of the data;
         o the nature of the data collected and the means by which it is collected;
         o whether the provision of the requested data is voluntary or required;
         o steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.
   b. Choice/Consent
      • Are options for opting in and/or opting out clearly explained?
      • If options for opting in and/or opting out do not exist, is this clearly indicated?
      • If choice/consent is limited (e.g., does not extend to third-party services) is this clearly explained?
c. Access/Redress

- Can an individual access data on himself or herself
- Can an individual contest the data's accuracy and completeness?
- If users have the ability to examine and/or revise their personal data, is the procedure clearly explained?
- If users do not have the ability to examine and/or revise their personal data, is this clearly indicated?
- What are the problems or limits to the user in accessing their personal data?

d. Integrity/Security

- Does the policy specify:
  
  i. how data is protected
  
  ii. who has access to the data
  
  iii. how long the data is kept
  
  iv. whether it is anonymized

- If data collected is to be used for research purposes, is that stated?

IV. Other aspects of content:

- Is the content of the policy accurate?
- Is the policy up-to-date (note last reviewed date)?
- Is it clear whether it is a policy or a procedure?
- Is it specific enough? Is it too specific?
- Do links to documents or other information sources referenced within the policy still work?

V. Disclaimers /scope

- Does the policy cover all relevant situations? If not, are exceptions clearly explained?
- Does the policy make clear when a third-party data provider is involved, and provide a link to the third-party entity’s relevant policies?
- Does the policy indicate how the involvement of third parties constrains the Library’s ability to control data content and use?

VI. Uniform policy requirements

- Is the policy’s “owner” (entity responsible for reviewing and updating) indicated by position or role, not by name?
• Is the entity that approved the policy, and subsequent revisions, identified? (Note: usually Administrative Council or Executive Committee for Library-wide policies.)
• Is the review cycle indicated (e.g., every year, every five years)?
• Are vague indications like “as needed” avoided?
• Are the dates of origin, approvals, revisions, and expiration all provided?

PART TWO: Other factors:

I. Is it in the right location on the website?
II. Is it in the right category in the policy index?
III. Is it linked from other appropriate web pages?
IV. Is it easily discoverable?
V. Is the “official” version available as a downloadable PDF?