



Shared Infrastructure, Shared Responsibility

CoreTrustSeal Board **Discussion Paper v1.0**

1. Introduction.....	1
2. Community as a Strength, Not a Shortcut.....	2
3. The Core Principle: Responsibility Cannot Be Fully Outsourced.....	2
4. What CoreTrustSeal Expects from Applicants Using Shared Infrastructure.....	3
4.1 Explicitly Identifies Shared Services and Partners.....	3
4.2 Exercises Responsibility for Curation and Preservation.....	3
4.3 Participates in Governance of Shared Systems.....	3
4.4 Retains Institutional Continuity.....	3
5. Conclusion.....	4

1. Introduction

Federated and consortium-based repository models are increasingly common across the digital preservation landscape. Communities pool resources to operate shared curation platforms, preservation pipelines, storage infrastructures, and access systems. These arrangements offer clear benefits: reduced duplication, lower costs, shared expertise, and greater sustainability.

At the same time, they raise important questions for trust certification. When members of a federated environment apply individually for CoreTrustSeal certification while relying on shared or outsourced functions, how should responsibility, accountability, and evidence of trustworthiness be transparently displayed and assessed?

This discussion paper articulates a CoreTrustSeal perspective on these questions, grounded in the principles of community stewardship, active preservation, and long-term responsibility. It builds directly on the CoreTrustSeal Extended Guidance¹ on third-party services and outsourced functions, clarifying how that guidance applies to federated preservation communities. The central argument is straightforward: shared systems are acceptable and often desirable, but responsibility for preservation cannot be transferred, diluted, or obscured. Certified repositories must demonstrate active, organizational responsibility for curation and preservation, even when those activities are operationally distributed.

2. Community as a Strength, Not a Shortcut

CoreTrustSeal explicitly recognizes that preservation is often a collective endeavor. Shared services, consortium governance, and federated infrastructures can strengthen repositories by:

- Enabling smaller or specialized organizations to meet preservation expectations
- Supporting consistency, interoperability, and shared standards
- Distributing expertise and operational risk
- Improving sustainability through shared investment

From a CoreTrustSeal perspective, using shared curation or preservation systems is not a liability; it is a legitimate operational model that must be made transparent, well-documented, and accountable.

3. The Core Principle: Responsibility Cannot Be Fully Outsourced

At the heart of CoreTrustSeal is a simple but non-negotiable principle: A repository may share systems, but it cannot outsource responsibility of their holdings. Community infrastructure must not become a substitute for institutional responsibility or accountability.

The CoreTrustSeal Extended Guidance is explicit about cooperation and outsourcing to third parties: *“The applicant remains responsible for ensuring that: the outsourced functions are carried out as agreed; roles and responsibilities are clearly defined and documented; evidence of compliance can be provided to reviewers; and the Designated Community can rely on the repository to preserve data and metadata for the long term. Outsourcing does not transfer responsibility; it only shifts operational duties.”*

Repositories that rely solely on shared infrastructure -- without internal capacity, oversight, or engagement -- do not meet the spirit of trustworthiness that CoreTrustSeal is intended to certify. If they do not, to some capacity, control the care given to their holdings, trust cannot be built in their services, as they have no influence on changes occurring to that care. It should instead be considered if the infrastructure used is in scope for their own CoreTrustSeal application.

¹ CoreTrustSeal Standards and Certification Board. (2025). CoreTrustSeal Trustworthy Digital Repositories Requirements 2026-2028 Extended Guidance (v01.00). Zenodo.

4. What CoreTrustSeal Expects from Applicants Using Shared Infrastructure

When evaluating CoreTrustSeal applications from members of a federated or shared infrastructure, reviewers should look for evidence that the applicant:

4.1 Explicitly Identifies Shared Services and Partners

Applicants must clearly identify all host organizations, partners, or third parties involved in CoreTrustSeal-relevant functions. Applicants don't need to disclose commercial or sensitive details, but should clearly describe the types of agreements in place. If multiple partners are involved, they should include a simple context diagram to clearly document the relationships. All such organizations should be clearly referenced under each relevant CoreTrustSeal Requirement.

4.2 Exercises Responsibility for Curation and Preservation

Applicants should demonstrate that they are not passive deposit points reliant solely on external partners to provide care to their holdings. While curation and preservation workflows may be implemented through shared systems, applicants must demonstrate active control over the parts of the data lifecycle they retain and evidence that the repository can evaluate and explain curation and preservation actions taken on its behalf. The key question is not who runs the system, but who is accountable for and has oversight over the curation, preservation and stewardship decisions. Ideally, such agreements on roles and responsibilities in the curation process are documented transparently and can be shared as evidence.

4.3 Participates in Governance of Shared Systems

Repositories applying for CoreTrustSeal should show meaningful engagement with the governance of shared infrastructure, including formal agreements, defined escalation paths for issues and failures, and input into system evolution and policy changes. Such participation signals both responsibility and organizational resilience.

4.4 Retains Institutional Continuity

Applicants must demonstrate that curation and preservation responsibility would persist even if the consortium changes structure, a shared service is replaced, or the repository exits the federated environment. This may include documented exit strategies, data portability provisions, or contingency planning. This type of planning is part of the concept of continuity of service, and is more important for applicants depending on shared infrastructures for their trustworthy services. It is important to document how members of the consortium or federation are informed about changes, updates, or risks, and how these are in turn communicated to the Designated Community.

5. Conclusion

CoreTrustSeal does not claim that federated and consortium-based repository models are less trustworthy. What this position paper aims to highlight is that trust should be anchored at the organisational level, ensuring that accountability remains visible and auditable, and that responsibility scales alongside infrastructure.

CoreTrustSeal can serve as a stabilizing framework that allows innovation in shared systems while preserving clarity about who is ultimately trusted. Shared systems are a strength. Shared responsibility is essential. But trust, ultimately, remains something each repository must earn and uphold by themselves.