Cultural Memory Lab Guide: Uploading Public Collections to IPFS with Storacha.network

A guide for community archives, libraries, and cultural organizations to prepare, upload, and share materials using Storacha, a beginner-friendly service for publishing to the IPFS network.

techsoup

GRAY AREA

About

The **Cultural Memory Lab** supports community archives, libraries, and cultural organizations in preserving shared histories using decentralized technologies. By leveraging tools like **IPFS** and **Filecoin**, we help participants make their public collections accessible, resilient, and independent of centralized platforms.

This guide walks you through how to prepare, upload, and share your first folder using **Storacha.network**, a beginner-friendly service for publishing to the InterPlanetary File System (IPFS), a decentralized network designed to preserve and share digital content reliably and long-term.

What You'll Learn:

- How to prepare and organize your files for decentralized storage
- What types of files are appropriate for IPFS — and which to avoid
- How to write a README.md file with helpful metadata and context
- How to upload your folder using Storacha and generate a CID
- How to share IPFS links generated by IPFS gateways on your website or project page
- How to explain your use of IPFS to different audiences
- Why decentralized storage is only one part of a resilient backup strategy

Step 1

Prepare Your Files for Upload

Choose a small collection (aim for 20) of non-sensitive files. Ideally, this comes from your existing archives; however, if you don't yet have enough suitable materials, you can create a sample folder instead.

Good examples include:

- Public domain images or scans
- Workshop notes or zines
- Sample datasets
- Oral history transcripts (publicly shareable)

Avoid uploading:

- Personal or sensitive data
- Copyrighted content you don't have permission to share
- Files that may need to be edited or removed later

Organize all files into one folder. You will upload this collection.

Step 2

Create a README.md File

Inside your folder, add a file called README.md. This should be a plain text file formatted using **Markdown syntax**. Markdown makes it easy to include headings, bullet points, and simple formatting that is readable both as raw text and on the web.

Clearly describing the contents of your folder is a key archival best practice. A well-written README file serves as a guide to your materials, offering essential context that supports long-term access and meaningful interpretation. Think of the README as a digital cover letter for your archive: it introduces the collection, outlines its purpose, and documents important metadata. The file helps future users — including community members, researchers, and archivists — understand what they're looking at and why it matters.

Good README files often include:

- A project description and scope
- Key dates and contributors
- A list of included files with titles, authors, and summaries
- Any usage rights or access restrictions

By following a consistent structure, you help ensure your archive is accessible and comprehensible, no matter who encounters it or when.

README.md File Example:

```
# Project Title: Uplifting Community Archives


**Description:**

This folder contains oral history transcripts collected by the Rising Voices Project in
Vancouver, BC. The collection documents personal stories from community members and aims
to support intergenerational knowledge sharing.


**Uploaded by:** Cultural Memory Lab Cohort, Spring 2025

**Date:** March 15, 2025

**License:** CC BY 4.0

**Contact:** hello@example.org


## File Listings


### 1. Transcript - Elder Leena

- **Title:** Elder Leena on Land and Language

- **Author:** Rising Voices Project

- **Date:** November 12, 2023

- **Summary:** A conversation with Leena about language loss, cultural resilience, and
youth education efforts in her community.
```

NOTE: We recommend that you also create an index.html file. This allows you to design a custom homepage for your archive — improving usability, context, and presentation.

See the appendix section: *Create an index.html Homepage for Your Archive.*

Step 3

Upload to Storacha.network

By using Storacha, your files will be uploaded to the IPFS network and made accessible through an **IPFS gateway** — a web-based tool that allows anyone to view and download IPFS content through a standard browser. This means your files can be opened without needing special software or a technical background. Gateways bridge the gap between decentralized networks and everyday web users.

There are many tools and services you can use to upload files to IPFS and Filecoin. We recommend starting with Storacha.network because it's simple, beginner-friendly, and doesn't require downloading special software.

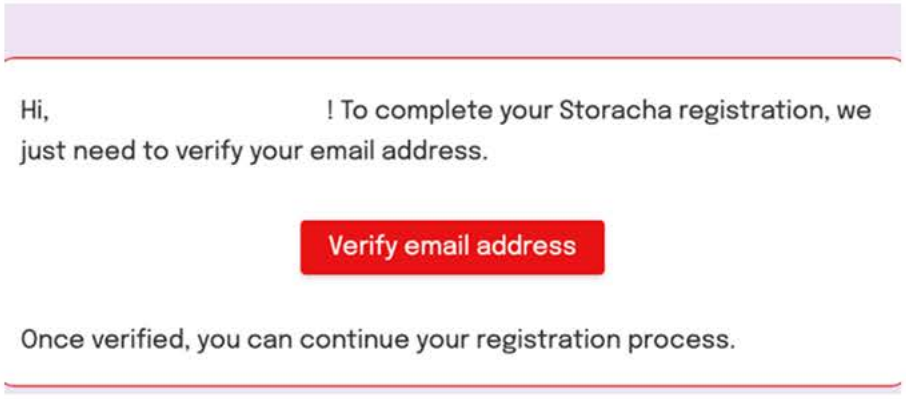
This step will generate a unique **CID (Content Identifier)** for your folder. CIDs act like permanent, verifiable web addresses. You can link to these CIDs from your website, emails, or project documentation — making your files accessible to anyone with a browser, even if they've never used IPFS before.

If you'd like to explore your IPFS content beyond browser gateways, you can use IPFS Desktop — a free, open-source tool that makes it easy to manage and share files from your own IPFS node.

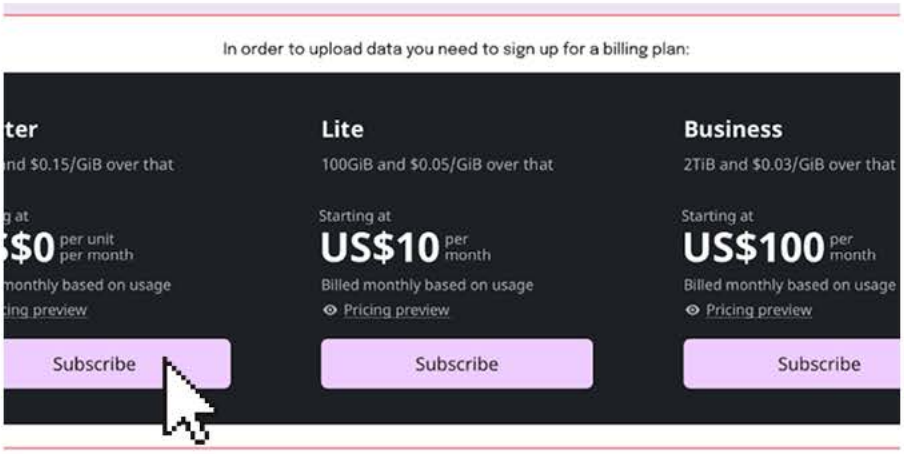
1. Go to Storacha.network and click Start Storing

2. Enter your email to verify your account

3. Click the verification link in your inbox



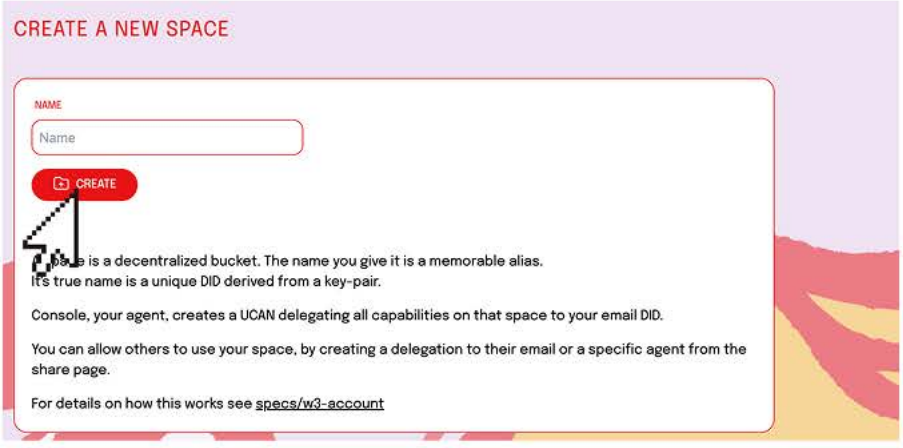
4. Select the Starter plan and click **Subscribe**



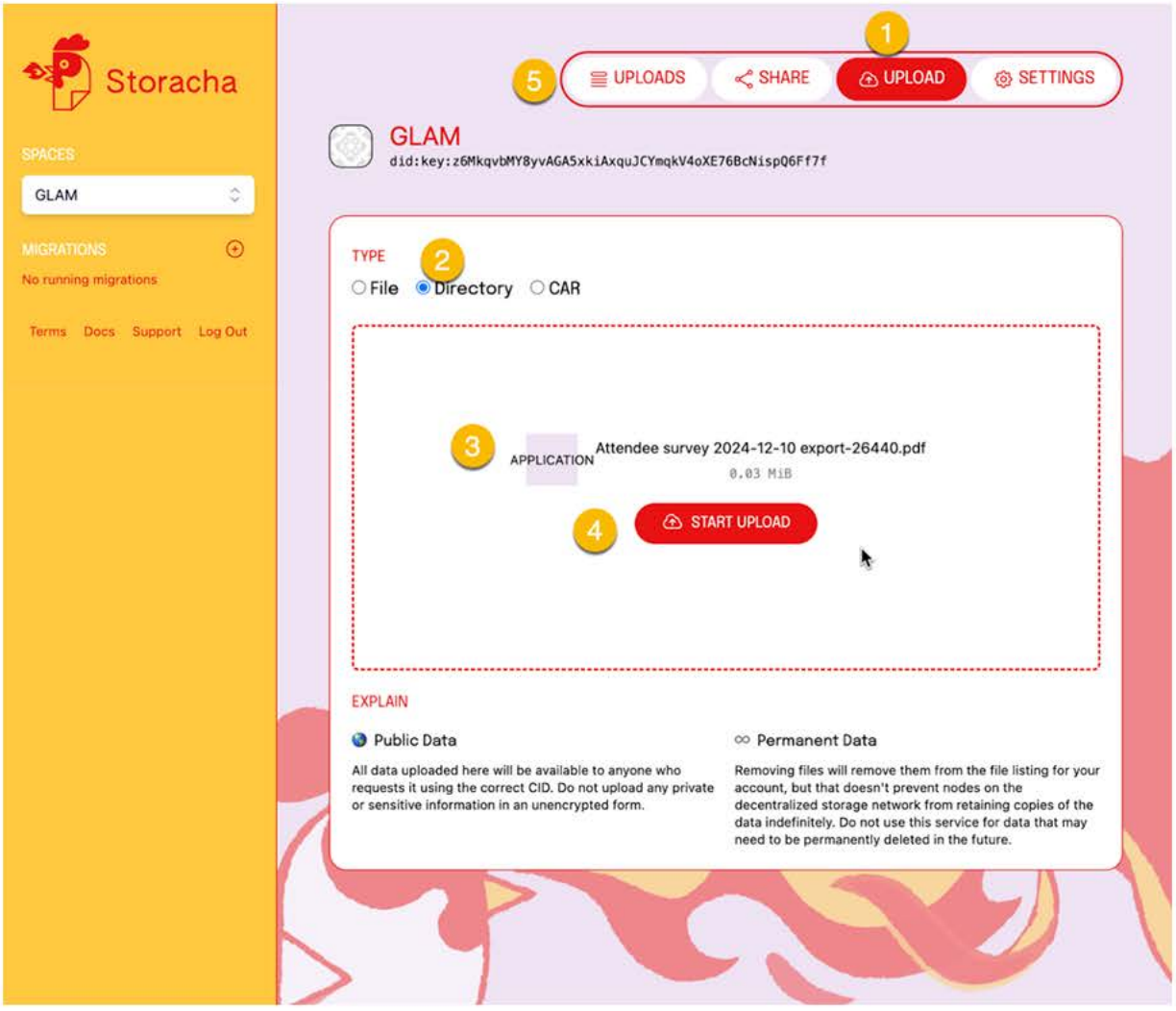
5. Add a payment method

Note: you won't be charged unless you go over the free 5 GB (this is very unlikely for 20 files, but you should double check the size of the files you are uploading to be certain).

6. Create a new Space (we recommend your project name)

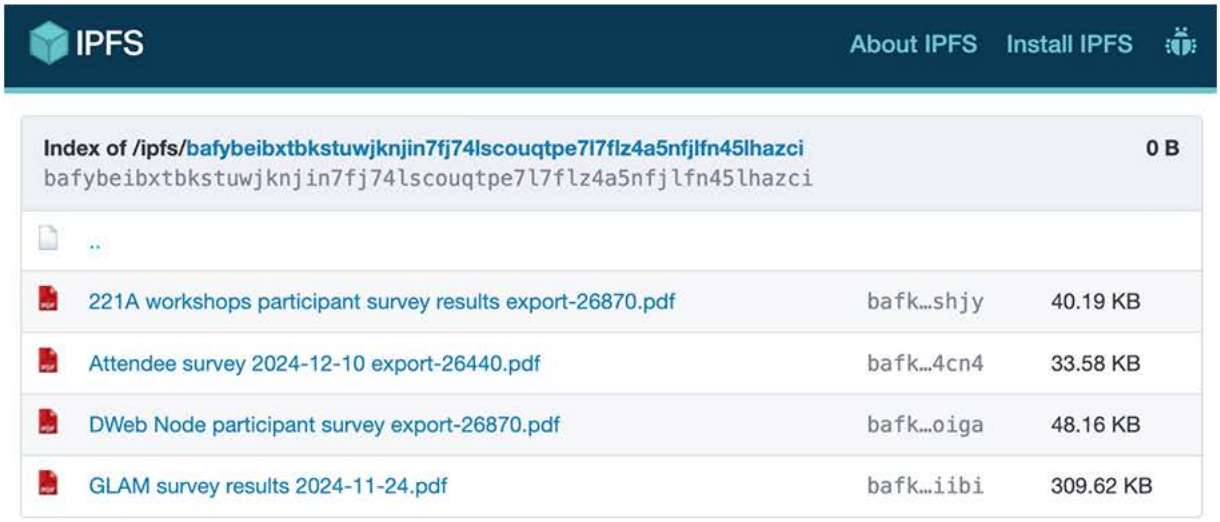


7. Click “Upload,” select “Directory” type, add your folder, and click “Start Upload.” Go to “Uploads” to see your folder.



8. Storacha will return a CID (Content Identifier)

9. Click the **URL** to open the Gateway, a webpage that can be accessed by any browser, making your files on IPFS and Filecoin accessible to those unfamiliar with IPFS.



NOTE: You can either share the folder OR individual files, which will have their own CIDs. To retrieve the IPFS gateway link for any of your individual files, right click and select Copy Link Address. Now that you have your IPFS gateway link you can add it to your existing websites or storage platforms.

10. Now that you have your IPFS gateway link, you can add it to your existing websites or storage platforms. Learn more about IPFS gateways here.

Add Links to Your Website or Project Page

You can use your IPFS gateway links anywhere you'd use a normal URL — embed them in project documentation, digital exhibitions, or blog posts.

Many people are not yet familiar with CIDs or IPFS, so it's helpful to include a short explanation alongside your links. This helps build understanding and trust with your audience, and provides context for why you're using decentralized storage.

For guidance, check the next section — “Write Your Own Why” — which includes example blurbs tailored for different audiences.

Example:

```HTML
<a
href="https://bafybeibwzif7e6spqdlvsjqdjz5pgibufp63rj3z3axlzftscs3gnjqb4u.ipfs.w3s.link/"
>View the files on IPFS</a>
```

Step 5

Write Your Own Why

Decentralized storage can feel technical — but it's also deeply values-driven. To help others understand your choice, consider drafting a short explanation.

Prompts:

- What does digital permanence mean to you?
- Why is it important that these files are accessible outside of centralized systems?
- How does IPFS align with your goals of equity, transparency, or community ownership?

Sample Language:

🧵 Short & Friendly
This file is stored on the InterPlanetary File System (IPFS), a decentralized network designed to preserve and share digital content reliably and long-term.

🌐 Website Blurb
We've archived this project on IPFS — a decentralized, peer-to-peer file storage network. Unlike traditional websites, files on IPFS are accessible as long as one person in the network continues to share them. That means even if our main site goes offline, this content remains available.

🌍 Values-Driven

Decentralized storage reflects our values: equity, autonomy, and access. By archiving our work on IPFS, we're joining a movement to build digital infrastructure that resists takedowns, enables community stewardship, and supports long-term memory for underrepresented stories.

📚 Preservation Statement

This project is preserved using IPFS (InterPlanetary File System) and Filecoin to ensure long-term access and resilience. We chose decentralized storage to reduce reliance on any single platform or server, and to support global access — especially in regions with censorship or connectivity challenges.

🛠️ Technical Rationale

IPFS offers content-addressable storage, meaning each file is identified by a unique cryptographic hash (CID). This ensures the integrity of the data over time. Paired with Filecoin's blockchain-based incentives, our storage is distributed, verifiable, and designed to persist independently of institutional hosting.

Step 6 Next Steps

Decentralized storage represents an exciting new approach to safeguarding our cultural memory — one that puts ownership and access in the hands of communities. By using IPFS and Filecoin, you're helping to shape a more resilient, inclusive, and participatory future for archiving.

This guide is just the beginning. We're grateful for your contributions and can't wait to see what you preserve and share.

In solidarity,

The Cultural Memory Lab Team, a project of TechSoup's Public Good App House

Appendix

Practice the 3-2-1-1-0 Backup Strategy

While decentralized tools like IPFS and Filecoin offer powerful new preservation options, it's important to remember that these are still emerging technologies. As such, we do not recommend relying on them as your only backup method.

Instead, consider IPFS to be one part of a broader **digital resilience strategy**, especially for preserving public, fixed-content materials. A modern, more comprehensive framework is the 3-2-1-1-0 backup strategy, which builds on traditional models to address modern threats like ransomware and incorporates the following principles:

- 3 = Maintain Three Copies of Your Data
  Keep one primary version and two additional backups to avoid a single point of failure.

- 2 = Use Two Separate Storage Media
  Store your backups on two different types of storage (e.g., cloud platform + external drive, or local server + IPFS). This provides protection from hardware or service-specific issues.

- 1 = Keep One Copy Offsite
  At least one backup should be stored in a geographically separate location to guard against local disasters (fire, flood, theft, etc.). Decentralized storage can play this role.

- 1 = Store One Copy Offline or Immutably
  To defend against ransomware or malicious deletion, one backup should be disconnected from the internet (air-gapped) or made immutable — meaning it cannot be altered or deleted. IPFS's content-addressed storage with cryptographic verification can support immutability.

- 0 = Ensure Zero Backup Errors
  Monitor and test your backups regularly. Run restore checks and make sure backups complete without errors so that you're ready if you ever need to recover.

What Types of Files Are Appropriate for IPFS?

While IPFS is ideal for many kinds of digital preservation, it's not suitable for everything. Below is a helpful guide to understand what works well — and what raises concerns:

Feature	Benefits	Concerns
Immutability	Files cannot be altered once uploaded, supporting historical accuracy.	Mistakes or sensitive data cannot be removed — important for personal or copyrighted files.
Verifiability	Files have a cryptographic hash (CID), so integrity can be independently verified.	Users must understand CIDs; verifying doesn't imply content validity or legal clarity.
Data Sovereignty	You can choose where and how to host content, outside of centralized control.	Requires technical confidence; some users may not understand where their data is hosted.
Vendor Lock-in Avoidance	Content can be accessed through any IPFS gateway or node.	Long-term access still depends on someone pinning the content or using Filecoin to guarantee availability.

Recommended File Types:

- Public reports, PDFs, zines
- Educational resources or toolkits
- Oral histories (with permission)
- Archival scans, photos, public datasets

Use Caution with These Types:

- Personal data (health, identity, contact info)
- Content subject to copyright
- Files that may need updates or takedowns

Tip: If in doubt, ask, "Would I feel comfortable making this content permanent and globally accessible?"

If not, consider local or encrypted alternatives instead of IPFS.

Addressing Authenticity and Provenance with the Starling Framework

Some digital content—especially evidence, testimonies, or archival material—may face questions about its **authenticity or provenance**. In these cases, decentralized storage alone may not be enough.

To strengthen trust, consider incorporating The Starling Framework — a methodology developed by the Starling Lab for capturing, storing, and verifying sensitive digital content.

The Starling Framework: Capture, Store & Verify:

- **Capture**: Use authenticated capture tools to embed secure metadata (such as timestamps and location data) at the point of creation.
- **Store**: Preserve content using cryptographic protocols and decentralized networks to ensure long-term integrity and replication.
- **Verify**: Register assets on an immutable ledger (like a blockchain) to allow for third-party verification of authenticity and provenance.

This approach is especially useful when working with **journalistic materials, human rights documentation, or fragile historical records**.

Create an index.html Homepage for Your Archive

This is an optional step, but recommended for projects teams with HTML skills.

When you upload a folder to IPFS, it is accessible through a public IPFS gateway. By default, visitors will see a basic file browser — a simple directory listing that works, but may not offer the best experience for viewers who are unfamiliar with IPFS or digital archives.

But there's a better way.

If your archive folder contains a file named index.html at the root level, IPFS gateways will automatically load and display it when someone visits your CID link. This allows you to design a custom homepage for your archive — improving usability, context, and presentation.

This optional technique is what powers more advanced "Data Lifeboat"-style archives, such as the Flickr Commons Lifeboat.

Benefits of using index.html

- Presents your archive with curated structure and visuals
- Enables navigation, context, and storytelling through HTML
- Offers an accessible, public interface — no IPFS knowledge required

How to serve an index.html file

- **Prepare your files:**
  Collect your archive materials and organize them in a folder. This is the folder you will upload to IPFS.

- **Create an index.html file:**
  Add a file named index.html to the root of your folder. This will serve as the home page when someone visits your archive via an IPFS gateway. You can choose from two options:
  - Use a simple HTML list of files.
  - Build on your existing README.md for structure and archive descriptions.

  Tips:
  - Always use relative links in your HTML (e.g., images/photo.jpg, ./file.pdf).
  - IPFS is case sensitive, so be sure the file names in your HTML code match the case of the actual files.
  - You may use a static site generator to help create the HTML.

- **Upload the file to IPFS:**
  Upload your folder (including your index.html file) to IPFS. After uploading, you'll receive a unique CID.

- **Access the file via the gateway:**
  Use a public gateway like https://<CID>.ipfs.w3s.link/index.html to view your site.

This Guide is supported by an award from the Filecoin Foundation for the Decentralized Web.

techsoup

GRAY AREA