THE NETWORKED CLASSROOM GUIDEBOOK

BUILDING A SANDBOX SOCIAL NETWORK FOR TEACHING SOCIAL MEDIA PRACTICE

Cameron McTernan

2026

The Networked Classroom Project and this guidebook

The networked classroom is a 3-year teaching-research project designed to incorporate simulated platform environments into communication and media degrees. This project responds to industry needs to enhance graduate competencies for social media technologies while addressing the issues of privacy and visibility on commercial social networking sites (SNSs). Using open-source technologies such Mastodon and activity-pub, this teaching intervention seeks to imbue skills in content creation, community management, brand building and ethics, whilst providing a private and secure environment for undergraduates to experiment with and develop their social media practice.

This guidebook is a practical, step-by-step resource designed for educators who want to teach social media skills using a sandbox social media environment. It shows you exactly how to build a private, completely secure web-based sandbox where students can learn by doing—and making mistakes—safely. This document outlines teaching philosophy behind the Networked Classroom and offers straightforward setup instructions. The guide also offers of classroom activities, including a live PR crisis simulation, organic brand-building projects, and student-led content moderation. Balanced with honest advice on managing server upkeep and student behaviour, this guide gives you the tools to run a highly engaging, ethically grounded media laboratory.

Table of Contents

Introduction: Reclaiming the Platform Sandbox

Modern communication and media education faces a foundational contradiction. To prepare graduates for a hyper-networked industry, curricula must offer hands-on experience with social media technologies, content strategy, algorithmic curation, and community management. However, conducting this training on commercial Social Network Sites (SNSs) forces an uncomfortable ethical compromise. It requires students to trade their personal data, digital privacy, and permanent public visibility for a course grade, all within algorithmic ecosystems designed for monetisation rather than learning.

The Networked Classroom offers a practical alternative to this dilemma.

Spanning three years of iterative teaching and research, this project introduces custom-built, simulated platform environments into higher education. By utilizing open-source, decentralised protocols—specifically Mastodon and ActivityPub—educators can deploy a fully functional, self-contained social media sandbox. This secure environment allows undergraduates to experiment freely, make tactical mistakes, and build authentic professional competencies without the external risks of commercial surveillance or public scrutiny.

What This Guidebook Offers

This guidebook is a comprehensive operational blueprint for higher education instructors, instructional designers, and educational technologists looking to replicate or adapt the Networked Classroom model. It bridges the gap between high-level platform theory and day-to-day classroom execution by providing:

Theoretical Grounding: A robust rationale for alternative digital pedagogies rooted in critical media literacy and platform capitalism.

Technical Blueprints: Concrete steps to deploy, lock down, and customize an independent Mastodon instance for institutional use.

Pedagogical Toolkits: Turnkey seminar activities, crisis simulations, and assessment frameworks designed to test student competencies in real time.

Ethical Guardrails: Honest reflections on the hidden labour of system maintenance, data governance within a university structure, and managing student behaviour in closed networks.

Guidebook Structure

The material is organized into five progressive modules, taking you from initial concept to live classroom deployment:

Module 1: Foundations & Philosophy

explores the ethical traps of commercial platforms in education and establishes the "pedagogy of the sandbox"—the theoretical framework supporting simulation-based learning.

Module 2: Architecture & Technical Infrastructure

provides the operational instructions needed to launch a Mastodon instance, configure it for absolute privacy (the "Isolation Protocol"), and manage student provisioning safely.

Module 3: Customization, Control, & Curation Tools

details how to modify the platform interface using alternative front ends and code forks, implement content moderation queues, and extract API data for student performance analytics.

Module 4: The Pedagogical Playbook

delivers structured lesson plans, including live PR crisis simulations, brand-building workshops, and platform governance exercises.

Module 5: Ethics, Frictions, and Drawbacks

confronts the practical challenges of this approach, analysing the technical overhead, the "uncanny valley" effect of a simulated network, and the institutional duty of care.

Module 1: Foundations & Philosophy

To understand why a simulated platform environment is necessary, we must first look at how social media is typically taught. For over a decade, the default approach in media education has been "live-fire" instruction: asking students to build public campaigns on X (formerly Twitter), manage live Facebook pages, or produce public-facing TikTok videos.

While well-intentioned, this approach overlooks a fundamental shift in the structure of the internet. It assumes that commercial platforms are neutral utilities. In reality, they are corporate enclosures.

1. The Commercial Platform Dilemma

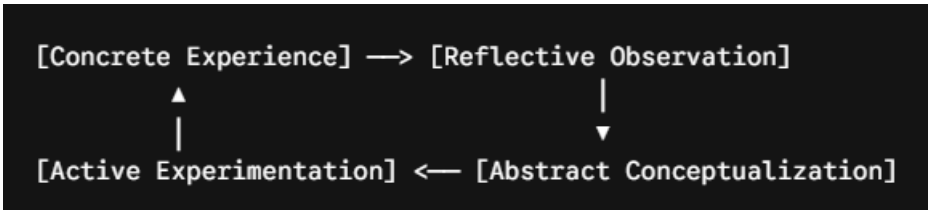
When we require students to use commercial Social Network Sites (SNSs) for coursework, we create an **institutional ethical trap**. This dilemma is built on three core systemic issues:

- **Forced Surveillance and Data Harvesting:** Students cannot complete their assignments without consenting to terms of service that strip them of data privacy. Universities inadvertently act as funnelling mechanism for corporate data collection, compelling students to trade their behavioural data for a course grade.
- **The Permanent Digital Footprint:** On public platforms, student mistakes are permanent. A poorly judged post, an unpolished graphic, or an experimental PR campaign can follow a student into the job market, indexed by search engines forever. This high-stakes environment chokes out genuine learning; when the cost of a mistake is reputational damage, students default to playing it safe.
- **Algorithmic Volatility:** Commercial platforms operate within algorithmic black boxes optimized for engagement and monetization, not pedagogy. An instructor cannot design a stable, repeatable learning experience when a sudden algorithm update or API restriction can wipe out a student project overnight.

The Ethical Imbalance: Higher education institutions operate under strict human-research ethics and student safety policies. Yet, the moment a student is required to log into a commercial platform to submit an assignment, those protections cease to exist.

2. Pedagogy of the Sandbox

The Networked Classroom addresses this trap through the **pedagogy of the sandbox**—a framework that privileges experiential learning within a failure-permissive environment.



When students operate inside a closed, open-source simulation, the pedagogical dynamic shifts fundamentally:

- **De-risking Failure:** In a private Mastodon instance, students can accidentally publish a broken link, mismanage a simulated PR crisis, or write an ineffective caption without real-world consequences. Lowering the stakes actually increases creative risk-taking and deeper technical engagement.
- **Decoupling from Algorithmic Anxiety:** In a commercial setting, students often conflate "good communication strategy" with "going viral." A simulated environment removes the distortion of the viral economy. Success is measured by strategic alignment, clarity, and ethical execution—not metrics driven by a hidden algorithm.
- **Transparency of Infrastructure:** Because open-source tools like Mastodon allow us to view and manipulate the environment, the platform itself becomes an object of study. Students don't just see the front-end user interface; they see how system settings directly shape human behavior.

3. Critical Digital Literacy Frameworks

Most industry training focuses entirely on **functional literacy**—knowing which buttons to press to schedule a post or optimize a headline. The Networked Classroom uses the sandbox to teach **critical digital literacy**, which views platform mechanics as deeply intertwined with political, economic, and social structures.

Our framework relies on three conceptual pillars:

Pillar	Focus	Classroom Reality
Platform Capitalism	Understanding how data ownership, hosting, and platform infrastructure translate into corporate power.	Moving students from passive consumers to infrastructure literate operators who understand the material costs of hosting and data storage.
Media & Algorithmic Diversity	Analyzing how specific platform architectures encourage or suppress diverse viewpoints, content forms, and marginalized voices.	Contesting the monoculture of commercial feeds by allowing students to see how a decentralized, chronological feed alters information flow compared to an engagement-driven algorithmic feed.
Data & Platform Governance	Exploring the mechanics of content moderation, community guidelines, and the labor required to maintain online civic spaces.	Transitioning students from simple content creators into platform governors who must actively interpret and enforce community standards.

By shifting the classroom from a corporate digital enclosure to an independent, open-source node, we transform social media education. We move away from simply training students to be compliant content production workers for the attention economy. Instead, we prepare them to be critical, ethical, and strategic leaders capable of navigating whatever platform architecture comes next.

Module 2: Architecture & Technical Infrastructure

Setting up the technical backbone of a simulated social media platform requires balancing data privacy, security, and administrative sanity. The goal is to create an environment that feels real to students but is sufficiently private that student practice is only visible to educators and their peers.

Please note, this section provides an overview on how to set up a private Mastodon server, which does require some basic understand of hosting webpages and web-applications. There is a reasonable skill-hurdle required to set this up, but for someone knowledgeable it can be set up within just a few hours. If you are considering starting your own Mastodon instance, we recommend liaising with your institutional IT team, but also taking advantage of the considerable resources available online about setting up a Mastodon server.

1. Hosting Ecosystems: Institutional IT vs. Managed Infrastructure

The first roadblock most educational projects hit is institutional procurement and security audits. Before choosing where to run your Mastodon server, weigh the long-term maintenance against the startup friction.

Hosting Model	Pros	Cons	Recommendation
Self-Hosted *(AWS, DigitalOcean, Institutional Iron)*	Total control over database, raw server logs, and code-level modifications (glitch-soc forks).	Heavy administrative overhead. Requires manual setup of Docker, PostgreSQL, Redis, SMTP email relays, and S3 media storage.	Use only if you have a dedicated DevOps engineer or educational technologist embedded in your department.
Managed Hosting *(e.g., Masto.host)*	Up and running in 15 minutes. Automatic daily backups, automated software updates, and scaling handled at the click of a button.	Slightly limited raw database access; requires asking support to toggle specific backend environment variables.	**Strongly Recommended.** For a 3-year research project, your time is better spent on pedagogy than managing database locks or email delivery failures.

2. The Isolation Protocol: Building the Sandbox

By design, Mastodon is built to "federate"—to connect and share data with thousands of other servers. For a classroom environment, you must intentionally break this core feature. Implementing the **Isolation Protocol** ensures that no student posts escape to the public internet, and no outside accounts can interact with your students.

To enforce absolute isolation, apply these three layers of defence:

Step A: Enable Limited Federation Mode

If you are self-hosting, add the following variable to your .env.production file. If you are using a managed host like Masto.host, email their support team to have this applied:

```
Code snippet

LIMITED_FEDERATION_MODE=true
```

What this does: This effectively turns your instance into a data silo. It switches Mastodon's federation model to an empty whitelist. Unless you explicitly authorize an external domain, your server will refuse all inbound and outbound connections.

Step B: Establish the Search Engine Wall

Ensure that accidental student visibility is blocked at the spider level.

1. In the Admin Dashboard, navigate to **Administration > Server Settings > Discovery**.
2. Uncheck **Opt into trends** and **Allow unauthenticated access to public timelines**.
3. Force a strict robots.txt rule at the server level to reject all web scrapers:

```
Plaintext

User-agent: *
Disallow: /
```

Step C: Close Public Registrations

You must lock the front door to prevent internet trolls or random users from signing up to your educational server.

- Go to **Administration > Server Settings > Registrations**.
- Set registrations to **Closed**. Accounts will only be created through administrative intervention.

3. Student Identity Management

How students log into the platform dictates your compliance with university privacy policies and your research data collection integrity. There are two distinct paths:

Path A: Institutional Single Sign-On (SSO)

Mastodon natively supports OAuth2, SAML, and OpenID Connect (OIDC). If your university IT allows it, you can hook the instance directly into the campus identity provider (like Microsoft Entra ID or Okta).

- *The Catch:* This forces students to use their real identities. It mimics an internal corporate network, which limits their freedom to experiment with pseudonymous brand-building or crisis simulation roles.

Path B: Pre-Generated Pseudonymous Batch Accounts (Recommended)

To maximize privacy and create a true simulation, decouple student identities from their real-world names entirely.

1. Create a secure master spreadsheet linking student IDs to generic handles (e.g., User_01, Strategist_A). Keep this offline and accessible only to the teaching team.
2. Use Mastodon's Command Line Interface (tootctl) to batch-create accounts via a simple terminal script, bypassing the need for students to verify via their personal emails.

By providing students with pre-activated credentials for a pseudonymous account on an isolated server, you insulate them entirely from the commercial internet. They enter the classroom not as private citizens risking their data, but as platform operators stepping into a professional simulation.

Module 3: Customization, Control, & Curation Tools

While vanilla Mastodon provides a robust out-of-the-box experience, it mimics a baseline microblogging structure. To transform it into a sophisticated teaching laboratory, we must layer on tools that allow students to experiment with design-driven user behaviour, handle content moderation at scale, and extract data for media analysis.

Because Mastodon relies on a decoupled API architecture, you don't install plugins through an administrative store. Instead, customization happens at the software-fork level or by leveraging alternative front-ends (separate user interfaces that talk to your server).

1. Advanced Server Tweaks: Deploying Glitch-soc

If your technical setup permits running a code fork, **glitch-soc** is an enhanced distribution of Mastodon that introduces several features critical to an educational sandbox.

- **Local-Only Posting:** This is a vital fail-safe feature. It allows students to write posts that are structurally blocked from ever leaving your local server, adding an extra layer of structural protection if your instance's isolation settings are ever misconfigured.
- **Rich Text and Markdown Support:** Vanilla Mastodon restricts posts to plain text. Glitch-soc enables native Markdown support. This lets students practice technical formatting, structure long-form micro-essays, and treat the text composition box like a professional content management system (CMS).
- **Thread Integrity Control:** It offers finer controls over who can reply to or interact with a post thread, which is highly useful when setting up restricted, student-run communication exercises.

2. Reshaping the Interface: Alternative Web Clients

One of the deepest critical media literacy lessons you can teach is how interface design drives user psychology. By introducing alternative front-end clients, you can host the exact same class dataset but radically change how students interact with it.

Two open-source clients stand out for classroom use:

- **Phanpy (phanpy.social):** Phanpy strips away the frantic, multi-column density of standard power-user layouts and focuses on visual layout clarity. It clusters consecutive replies from the same user into "sub-threads" and groups algorithmic-free trends into clean, digestible widgets.
- **Elk (elk.zone):** Elk provides a slick, modern interface that mimics high-end commercial apps like Threads or Bluesky.

The Pedagogical Experiment

Have half the class interact with the sandbox via the traditional Mastodon multi-column dashboard, while the other half uses Phanpy's minimalist interface. After a live posting exercise, bring them together to discuss how the visual layout of their feeds directly influenced their posting speed, reply frequency, and overall sentiment.

3. Content Governance & Analytics Curation

Managing the backend of your network isn't just an administrative chore; it is an active data tracking laboratory.

Implementing Keyword & Regex Filters

Use the **Administration > Content Moderation** suite to build structural rules that simulate automated content filters or platform boundaries:

- Set up keyword warning queues where posts containing specified words are automatically routed to a moderation queue before going live. This simulates the algorithmic filter structures used by massive corporate Trust & Safety teams.

Extracting Data for Analytical Curation

Because Mastodon exposes comprehensive API endpoints, you do not need to scrape pages to analyse class behaviour. Students can act as data scientists, querying the platform to analyse metrics like network density, post-concentration patterns, or structural diversity in information flows.

Instructors or students can use a basic Python script via the Mastodon.py library to extract raw json data from their own sandbox server for media research assignments:

```python
from mastodon import Mastodon

# Initialize API connection to your secure sandbox
mastodon = Mastodon(
    access_token='your_admin_production_token',
    api_base_url='https://your-classroom-instance.local'
)

# Fetch the local timeline activity for student analysis
public_tweets = mastodon.timeline_local(limit=40)

for post in public_tweets:
    print(f"User: {post['account']['username']}")
    print(f"Content: {post['content']}")
    print(f"Replies: {post['replies_count']} | Boosts: {post['reblogs_count']}\n---")
```

By pairing this programmatic data extraction with their daily usage, students move beyond basic content creation. They can map out interaction networks, track which internal accounts command the most visibility, and critically evaluate how platform architecture shapes digital influence.

Module 4: The Pedagogical Playbook

This module translates platform theory into specific, live classroom exercises. Because the sandbox is private and isolated, you can run high-stakes scenarios that would be impossible or dangerous to execute on the public internet.

The following three turnkey activities are structured to run over a multi-week semester block, building student skills from content strategy up to infrastructure governance.

Activity 1: The Live PR & Misinformation Crisis

- **Objective:** Train students to manage rapid-response communication and mitigate misinformation under intense cognitive load.
- **The Secret to Success:** Do not tell students to simply "pretend" there is a crisis. You must actively seed the simulation. The teaching team should use a handful of pre-arranged auxiliary accounts to act as "adversarial injectors" (trolls, leak accounts, or aggressive journalists) to drive the narrative forward in real time.

Simulation Roles

To run this effectively, split your seminar into three distinct operational teams:

Team	Core Objective	Key Actions
Corporate Comms	Protect organizational reputation and maintain a single source of truth.	Issue official statements, monitor the local timeline, and answer stakeholder queries.
Investigative Journalists	Uncover the truth, interview stakeholders, and break news stories.	Publish live updates, pressure corporate accounts for answers, and verify leaked files.
The Public / Inbound Catalysts	Simulate consumer sentiment, amplify panic, or spread unverified rumors.	Share organic reactions, boost sensational posts, and tag corporate accounts demanding action.

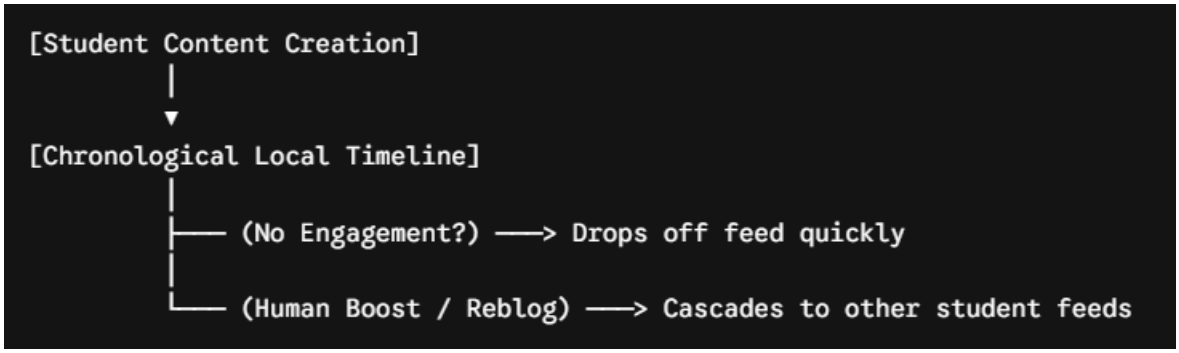
The 90-Minute Run Sheet

1. **Minute 00–15 (The Trigger):** A whistleblower account posts a leaked internal document or a pixelated photo suggesting an environmental spill or data breach tied to the corporate team's brand.

2. **Minute 15–45 (The Amplification):** The Public team starts boosting the leak. Investigative Journalists begin tagging the corporate brand asking for immediate comment.
3. **Minute 45–70 (The Mid-Point Inject):** The teaching team drops a piece of genuine *misinformation* into the feed (e.g., an altered image showing a secondary disaster). The corporate team must identify the fake, debunk it publicly, and keep their original crisis messaging stable.
4. **Minute 70–90 (The Cool-Down & Debrief):** Freeze the instance timelines. Gather the class to analyze the propagation chain using the local timeline feed.

Activity 2: Strategic Brand Building (No Algorithmic Aid)

- **Objective:** Teach students content strategy, community engagement, and organic copywriting without relying on paid amplification or a recommendation engine.
- **The Challenge:** On modern commercial sites, algorithms push content into users' feeds based on optimization metrics. On a chronological, decentralized Mastodon instance, content only travels if human beings choose to interact with it, boost it, or follow the account.



The Assignment Design

Assign each student (or small group) a niche brand persona (e.g., a sustainable local cafe, a public health initiative, or an indie gaming studio). Over four weeks, they must execute a full content calendar within the instance.

- **The Requirement:** They must post 3–5 times per week using varying content formats (threaded micro-blogs, visual assets, polls).
- **The Interaction Rule:** Students cannot just broadcast; they must spend 30% of their time interacting with other student brands, building logical cross-promotional partnerships, and replying to community posts.

- **The Assessment Metric:** Success is graded on *structural depth* rather than raw follower count. Students submit a reflective portfolio demonstrating how they adapted their copywriting, hash-tagging, and visual layouts to capture attention in a purely chronological information ecosystem.

Activity 3: The Trust & Safety Council

- **Objective:** Transition students from platform consumers to platform governors by forcing them to make difficult content moderation choices.
- **The Setup:** Midway through the semester, deliberately instruct a small, select group of advanced students to post content that deliberately tests the boundaries of the instance's pre-defined Acceptable Use Policy (AUP)—such as highly polarizing political takes, uncredited artwork, or ambiguous spam.

The Execution Workflow

1. **The Flagging Phase:** Instruct the rest of the class to use Mastodon's native "Report" tool whenever they encounter content that makes them uncomfortable or seems to violate community standards.
2. **The Council Convening:** Form a rotation of 4–5 students to act as the "Trust & Safety Board" for the week. They log into the Admin Dashboard and review the moderation queue.
3. **The Adjudication:** For each flag, the council must debate and choose a concrete platform action:
    - *Dismiss the report* (protecting expression).
    - *Apply a Content Warning (CW)* (remediating context).
    - *Delete the post or suspend the user* (enforcing safety).

The Critical Reflection: The final assessment for this module requires students to write an essay defending their moderation decisions against their university's broader speech guidelines. This strips away the abstraction of "free speech online" and forces them to confront the material, legal, and operational labour of online community governance.

Module 5: Ethics, Frictions, and Drawbacks

No educational innovation comes without a cost. While building an independent, isolated platform sandbox solves the ethical traps of data surveillance and reputational risk, it introduces a completely new set of operational frictions and institutional responsibilities.

Running *The Networked Classroom* means transitioning from a traditional instructor into a combination of server administrator, platform regulator, and community manager. This final module addresses the hidden challenges, systemic limitations, and ethical responsibilities of managing a simulated network.

1. The "Uncanny Valley" of Simulated Social Media

The biggest pedagogical limitation of a closed network is scale. A live commercial platform derives its energy, volatility, and strategic difficulty from its massive user base, unpredictable algorithmic shifts, and chaotic public commentary.

A closed classroom instance with 50 to 150 students can easily fall into an **uncanny valley**—a simulation that looks like a platform but lacks the structural dynamics of a real network.

- **The Echo Chamber Effect:** Without an influx of outside users, the local timeline can quickly become stale or hyper-predictable. Students know exactly who is behind every account, which can cause them to slip into overly polite or performative interactions rather than testing genuine strategic communication.
- **The Metric Deficit:** In a small network, a student's post might only get three or four boosts (retweets). For students accustomed to the instant validation of corporate algorithms designed to hook their attention, this lower engagement can feel demotivating.
- **Mitigation Strategy:** Instructors must act as an artificial environment engine. You cannot just launch the server and walk away. You must actively introduce systemic friction—such as deploying automated bots to post external news feeds, bringing in students from previous cohorts to act as outside agitators, or utilising the live injections outlined in Module 4.

2. Duty of Care in Closed Spaces

Paradoxically, removing the risks of the public internet can sometimes lower students' behavioural inhibitions too much. When students know an environment is private, unindexed by Google, and protected by an institutional safety net, their online behaviour can shift unpredictably.

The Sandbox Paradox: Lowering the stakes to encourage experimentation can inadvertently create a space where students feel insulated from the real-world consequences of communicative harm.

During a multi-year project cycle, you will likely encounter two behavioural archetypes that require intervention:

- **The Overly Edgy Role-player:** In simulations involving politics, PR crises, or platform governance, students testing boundaries may cross the line into genuine harassment, hate speech, or toxic trolling under the guise of "just playing a character."
- **The Academic Disengagement:** Conversely, some students may view the private server as a trivial, inconsequential task compared to writing a traditional essay. They may post low-effort content or spam the timeline to simply meet their weekly posting quotas.

Enforcing the Framework

Your institutional duty of care does not disappear because the platform is private. The student-run Trust & Safety Councils discussed in Module 4 must always be backed by the university's overarching student code of conduct. The guidebook recommendation is clear: **Before the instance launches, students must sign an operational agreement stating that while creative risk-taking is encouraged, the sandbox remains an official university learning space subject to standard behavioural policies.**

3. The Invisible Labor of Platform Maintenance

The academic economy rewards research outputs and curriculum design; it rarely accounts for the hidden, ongoing labour of technical system maintenance. Operating an open-source platform layer requires a distinct commitment of time and technical maintenance.

Maintenance Category	Task Breakdown	Estimated Overhead
Identity & Access	Resetting lost passwords, managing manual account provisioning, troubleshooting student login failures.	2–3 hours per week (Peak at start of term)

Data & Storage	Monitoring server disk space, clearing cached remote media assets, ensuring automated database backups are functioning.	1 hour per week
Software Lifecycles	Upgrading the Mastodon core code to patch security vulnerabilities, fixing broken database migrations after updates.	4–6 hours per semester block
Content Moderation Escalation	Acting as the supreme court of the platform when student moderation councils split on a decision or when an incident requires official intervention.	Variable (Ad hoc)

If you are a solo researcher or an adjunct instructor without direct, institutional support from educational technologists or systems administrators, this technical overhead can quickly overwhelm your teaching time.

Moving Forward: The Infrastructure Imperative

The frictions outlined in this module are not reasons to abandon the project. Instead, they are proof of its importance.

By confronting the realities of server maintenance, dealing with the complexities of content moderation, and experiencing the limitations of small-scale networks, both you and your students are engaging with the true mechanics of contemporary digital media. *The Networked Classroom* pulls back the polished curtain of platform capitalism. It demonstrates that social media networks are not magical, neutral conduits for human connection—they are fragile, expensive, highly managed technical and social infrastructures that require active, ethical, and deliberate governance to survive.