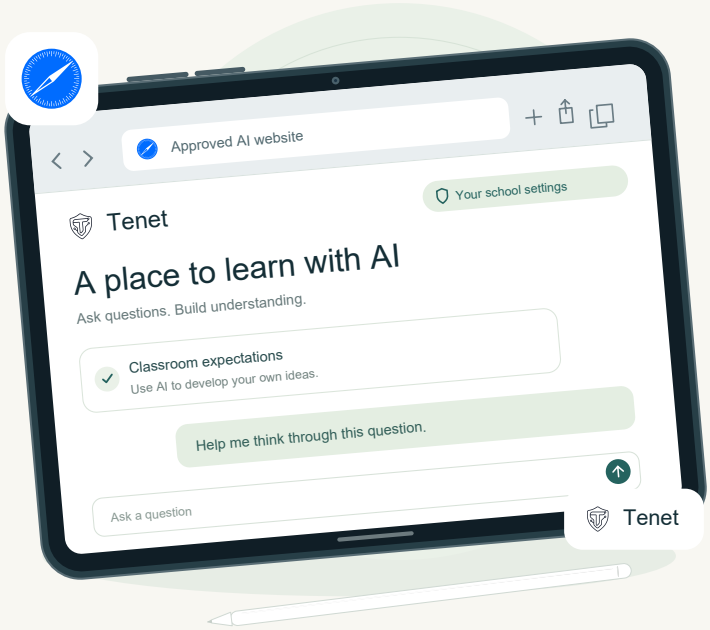
School AI rules on iPad

Students use Safari with Tenet. Teachers set class rules from their laptop. Your school keeps configured reports in its own cloud storage.



01 **School setup** → 02 **Safari + Tenet** → 03 **Teacher rules** → 04 **School reports**

Your school sets it up once

Your IT team installs Tenet and connects it to your school's settings.

IT enables the Safari extension, allows access to approved AI websites, and helps students sign in with their school accounts. Students then open supported AI websites in Safari as part of their normal classwork.

We confirm the app, devices, and school setup together during an iPad pilot.

The right browser
Simple teacher controls

Safari

Student AI use

Open approved AI websites with Tenet active.

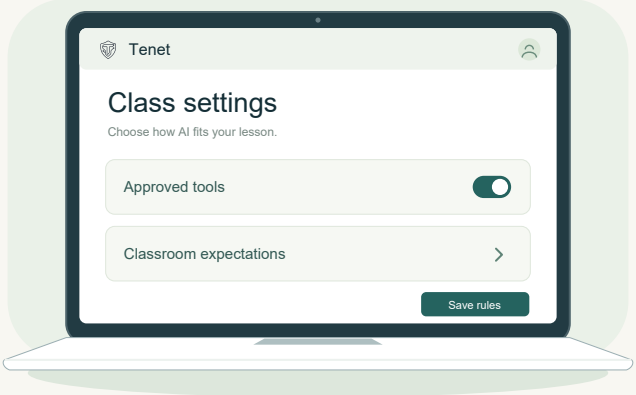
Chrome

Managed separately

School IT can block AI sites through Chrome policies.

Schools can block selected AI websites in managed Chrome using Google Admin URL blocking. This lets the school keep approved student AI use in Safari with Tenet. IT also manages unapproved browsers and native AI apps separately.

Teachers work from their laptop



With the school-approved Tenet extension installed in their browser, teachers sign in and open the Tenet dashboard.

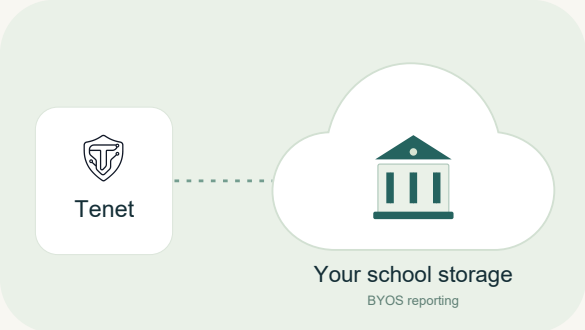
1 Choose the class

2 Adjust permitted rules

3 Save the changes

Teachers choose from district-approved AI platforms and settings they are authorized to change. Saved rules synchronize to connected, authenticated student devices. The teacher does not configure each iPad individually.

Reports in your school's storage



BYOS means Bring Your Own Storage. Your school connects Amazon S3, Google Cloud Storage, or Azure Blob Storage. Tenet sends the configured usage and incident records to that school-owned destination.

Your school controls access, retention, and deletion. Records can include student and class identifiers. Optional redacted prompt excerpts require district opt-in. Authentication, policy delivery, and alert services remain separate parts of Tenet.

Choose a practical guide

01 Set up school iPads

TestFlight, Safari and school management

02 Manage AI access in Chrome

Student groups, blocked URLs and checks

03 Set up teacher laptops

Chrome, Safari and staff PII protection

04 Connect school-owned reporting

Cloud storage and help from Tenet

Start small: test Safari access, Chrome restrictions, one saved teacher rule, reporting delivery, and recovery after restarting an iPad.

Set up school iPads

Guide 1 | Start with an agreed school pilot

1 Confirm the pilot with Tenet

Your IT team installs Tenet and connects it to your school's settings. Agree the iPad models, operating systems, school accounts, approved AI sites and management setup. Receive the school's Tenet invitation.

2 Install Apple TestFlight

Install Apple TestFlight on the approved test iPad. TestFlight is the pilot delivery route; the production distribution route is agreed with school IT.

3 Accept the invitation and install Tenet

Open the invitation on that iPad. Select **View in TestFlight > Accept > Install**. Returning testers use **Update**. Open Tenet after installation and follow its activation guidance.

4 Enable Tenet in Safari

Open **Settings > Apps > Safari > Extensions > Tenet**, then turn on **Allow Extension**. If school management locks this setting, IT makes the change.

5 Allow the approved websites

Grant Tenet access to the school-approved AI websites. Check that the extension is enabled in the Safari profile students actually use. Open an approved AI website in Safari.

6 Sign in and verify the school setup

Open Tenet from Safari's extension menu and sign in with the authorized school account. Confirm the correct school or class, test an allowed and a restricted interaction, then restart Safari and repeat the check.

For centrally managed iPads

IT deploys the approved app through its agreed channel and configures extension enablement and website permissions. Apple's managed extension controls require supervised iPads on iPadOS 18 or later. Tenet's current configuration route uses **ExtensionConfigs on iPadOS 18.4 or later**; deliver settings to the extension, not only its app. Confirm this with the MDM provider and Tenet.

TestFlight builds are available for up to 90 days. Keep the pilot build current; do not rely on an expired beta for school access.

TestFlight help | Enable iPad Safari extensions | Apple managed Safari settings

Manage AI access in Chrome

Guide 2 | Apply student restrictions while preserving teacher access

1 Open the Chrome settings in Google Admin

Sign in to admin.google.com with the required administrator privileges. Open **Devices > Chrome > Settings > User & browser settings**. Some Chrome Enterprise Core views use **Chrome browser > Settings**.

2 Select the student organizational unit or group

Apply the restriction to the pilot student OU or group. Keep teachers in their intended staff cohort. Review inherited settings and group overrides so the student policy does not unintentionally block teacher workflows.

3 Add the AI websites to block

Open **Content > URL Blocking**. Under **Blocked URLs**, enter the selected domains, one per line. Review **Blocked URL exceptions** for entries that would allow those sites.

Example domains

chatgpt.com • chat.openai.com • claude.ai
gemini.google.com • copilot.microsoft.com

4 Save and check the student browser

Select **Save**, then restart Chrome on a pilot device. Open **chrome://policy**, select **Reload policies**, and confirm the expected **URLBlocklist** value and status. Policy changes can take time to reach devices.

5 Test both student and teacher access

Visit a blocked AI site in student Chrome. Verify that the same intended site still opens in Safari with Tenet. Check an authorized teacher account separately. If staff need an exception, configure it deliberately at the correct staff OU or group and retest.

Chrome on iPad needs its own management setup

For user policies, enable management for signed-in Chrome users and **Chrome on iOS > Apply supported user settings**; the student must use the managed school account. Alternatively, use the school's supported Chrome MDM enrollment. Confirm each setting supports iOS. Test signed-out and personal-account behavior; use MDM controls for unapproved browsers or native AI apps.

Maintain the domain list as services change. Blocking broad domains such as google.com or microsoft.com can disrupt unrelated school services.

Google URL blocking | URL syntax | iOS user policies | iOS MDM enrollment

Set up teacher laptops

Guide 3 | Install the approved extension and confirm the teacher role

Chrome on Windows or Mac

For teachers: use school-managed Chrome and the Tenet channel assigned by IT. If the school uses the Chrome Web Store edition and permits self-installation, open the school-approved Tenet listing and select **Add to Chrome > Add extension**. Otherwise, IT installs it for you.

For IT deployment: in Google Admin, go to **Devices > Chrome > Apps & extensions > Users & browsers**. Select the teacher OU or group, then **Add > Add Chrome app or extension by ID**. For the self-hosted channel, enter the district-assigned Tenet ID and choose **From a custom URL** with the assigned update-manifest URL. Set **Installation policy > Force install** and **Save**. Use the supplied **updates.xml** feed, not a versioned CRX file.

Restart Chrome, open the Extensions menu, and pin Tenet if desired. Open Tenet and sign in with the authorized school teacher account.

Safari on a Mac laptop

Install the school-provided Tenet Safari app through the agreed school or TestFlight pilot channel. In Safari, open **Safari > Settings > Extensions** and select the checkbox for Tenet. Select Tenet, choose **Edit Websites**, and allow the approved AI domains. Confirm the extension is enabled in the Safari profile being used. Open Tenet and sign in with the authorized school account.

Open the class and save a rule

Open Tenet's dashboard, select the assigned class, adjust a permitted instruction, mode or approved AI platform, and select **Save class rules**. Confirm the change on a connected student device. Class management requires the correct teacher role and class assignment; having staff DLP alone does not grant class access.

Protecting personal information

When staff data loss prevention (DLP) is enabled by the district, Tenet checks prompts and supported file uploads on supported AI websites for personal information such as email addresses, phone numbers, SSNs and student identifiers. School policy determines whether the teacher reviews a redacted version, receives automatic redaction, or is blocked. Some policies permit an explained override; hard blocks cannot be overridden.

Protection applies in the enabled browser and supported AI workflows, not every app or file on the laptop. Confirm it with a school-approved test using invented sample details.

Google extension deployment | Manage desktop Chrome | Apple Safari extension setup

Connect school-owned reporting

Guide 4 | Work with school IT, Caleb and Tenet to verify delivery

1 Choose the school-owned destination

Select an **Amazon S3 bucket**, **Google Cloud Storage bucket**, or **Azure Blob container** in the school's cloud account. Google Cloud Storage is different from a Google Drive folder. Agree region, retention and who can read reports.

2 Plan the connection with Tenet

Share the chosen provider, school or district identity, device-management setup and reporting needs with Caleb and Tenet. We can help map the configuration, work through the provider setup with your IT team, and plan the connection checks. The school retains cloud ownership and access control.

3 Separate writing from staff reporting access

IT provisions the required writer permissions for the approved destination and delivers configuration through the school's management system. Configure authorized staff reader access separately. Student devices must not receive staff reporting credentials.

4 Configure the reporting provider

An authorized admin opens **Analytics, Alerts & Data Connections** in Tenet. Select the appropriate **Amazon S3 / GCS** or **Azure Blob** setup. The S3/GCS setup wizard helps distinguish managed writer settings from device-local reader settings. Save the analytics sync settings.

5 Test the connection and a real reporting flow

Run **Test Connection** and confirm the destination accepts a write. Where authorized reader access is configured, verify the read check too. Then create school-approved test activity and confirm the expected record reaches the correct school destination. A connection probe alone does not prove activity reporting.

6 Check access, retention and ongoing operation

Confirm that only authorized staff can read reports and that the cloud retention and deletion rules match the school's choices. Verify live reporting after sign-in and an iPad restart. Connectivity and an active authenticated session are needed for live reports and new policy updates.

What the school should agree

Configured records may include student and class identifiers. Optional redacted prompt excerpts require district opt-in. BYOS is the reporting destination; Tenet's authentication, policy delivery and alert services remain separate.

For setup coordination: caleb@truemadeai.com | ipads.truemadeai.com