Recommended Standard Student MDM Profile

This guide provides a recommended baseline configuration for **student Apple devices** managed through **Mosyle MDM**. Student devices should be configured with stronger restrictions than teacher or staff devices because they are used in a classroom environment, may be shared or assigned to minors, and must support school safety, security, and compliance requirements.

> **Recommended Profile Name:**
> `Students – Standard Restrictions and Security`

Purpose

This profile should be applied to school-owned student iPads, MacBooks, and other Apple devices. The goal is to keep the device focused on learning, reduce distractions, protect students, prevent unauthorized changes, and maintain consistent device behavior across the school.

- Keep devices focused on instructional use
- Reduce classroom distractions
- Prevent inappropriate sharing or communication
- Protect student data and school-owned equipment
- Support web filtering and school compliance requirements
- Prevent students from bypassing school controls

Recommended Mosyle Profile Naming Examples

```
Students - iPadOS - Standard Restrictions
Students - macOS - Standard Restrictions
Students - Security Baseline
Students - Web Filtering
Students - App Controls
Students - Shared Device Restrictions
```

Recommended Baseline Settings

1. USB Storage / External Drives

> **Recommendation:** Block USB storage and external drives for students unless there is a documented instructional exception.

Setting	Recommendation
USB storage access	Blocked
External drives	Blocked unless approved
Unknown USB accessories	Restricted
File transfer to removable media	Not allowed

Students should not be able to copy school files, screenshots, assignments, or sensitive information to removable storage without approval. External storage also increases the risk of malware, inappropriate files, and data loss.

2. Siri and Dictation

> **Recommendation:** Disable Siri and restrict Dictation unless required for accessibility.

Setting	Recommendation
Siri	Disabled
Siri while locked	Disabled
Siri Suggestions	Disabled
Dictation	Disabled unless required for accessibility

Siri is not normally required for student learning devices and can create privacy concerns, classroom distractions, or unintended lock-screen access.

3. AirDrop

> **Recommendation:** Disable AirDrop for all student devices.

Setting	Recommendation
AirDrop	Disabled
AirDrop receiving from Everyone	Not allowed
Password sharing through AirDrop	Disabled

AirDrop should be disabled for students because it can be used for inappropriate file sharing, classroom disruption, bullying, image sharing, or bypassing normal communication controls.

4. Apple ID and iCloud

> **Recommendation:** Block personal Apple ID use and limit iCloud services.

Setting	Recommendation
Personal Apple ID	Blocked
Managed Apple ID	Allowed if school-managed

Setting	Recommendation
iCloud Drive	Disabled unless required
iCloud Photos	Disabled
iCloud Keychain	Disabled
iCloud Backup	Disabled unless school-approved

Student devices should not be tied to personal Apple IDs. Personal accounts can create privacy issues, app ownership problems, Activation Lock concerns, and support issues when the device needs to be reassigned.

5. App Store and App Installation

> **Recommendation:** Students should not install apps directly. Apps should be deployed through Mosyle.

Setting	Recommendation
App Store	Disabled or restricted
Install apps	Not allowed by students
Remove apps	Not allowed for managed apps
In-app purchases	Disabled
Untrusted enterprise apps	Blocked

Required apps should be assigned through Mosyle and Apple School Manager Apps and Books. This keeps app licensing, installation, updates, and removal under school control.

6. Classroom Distraction Controls

> **Recommendation:** Disable non-instructional features that create distractions or safety concerns.

Feature	Recommendation
Game Center	Disabled
Messages	Disabled unless required

Feature	Recommendation
FaceTime	Disabled unless required
Music / Apple Music	Disabled or restricted
Podcasts	Disabled or restricted
News	Disabled or restricted
Screen recording	Restricted unless needed for instruction

7. Camera, Microphone, and Screen Recording

> **Recommendation:** Allow only when instructionally needed.

Feature	Recommendation
Camera	Allowed if needed for instruction
Microphone	Allowed if needed for instruction
Screen recording	Restricted unless approved
Screenshots	Restrict if supported and appropriate

For many classrooms, the camera and microphone may be required for projects, testing, accessibility, video assignments, and teacher-approved activities. These should not be blocked globally unless the school has a specific reason.

8. Web Filtering and Content Protection

> **Recommendation:** Student web filtering should be required on all student devices.

Category	Recommendation
Adult content	Blocked
Malware / phishing	Blocked
Proxy / VPN bypass sites	Blocked
Gambling	Blocked

Category	Recommendation
Violence / weapons	Blocked according to school policy
Social media	Blocked or limited by grade level
YouTube	Restricted or education-filtered
AI tools	Controlled by school policy

Student filtering should apply both on-campus and off-campus when possible. Students should not be able to bypass filtering by using VPN apps, proxy sites, alternative browsers, private relay services, or unauthorized DNS settings.

9. Browser and Search Settings

Setting	Recommendation
Safari	Allowed only with filtering
Private Browsing	Disabled where possible
Browser extensions	Restricted
SafeSearch	Enforced
YouTube Restricted Mode	Enforced where applicable

10. VPN, DNS, and Network Changes

> **Recommendation:** Students should not be allowed to install VPNs, modify DNS, or bypass network controls.

Setting	Recommendation
VPN apps	Blocked unless school-managed
DNS changes	Restricted
Proxy configuration	Restricted
Private Relay	Disabled

11. Privacy and Security

> **Recommendation:** Enforce security settings on all student devices.

Security Item	Recommendation
Password / Passcode	Required based on grade level and device type
Auto-lock	Required
FileVault on macOS	Enabled for assigned MacBooks
Firewall on macOS	Enabled
Gatekeeper	Enabled
Local admin rights	Not allowed

12. Account and Settings Restrictions

Setting	Recommendation
Account changes	Restricted
Erase all content and settings	Blocked
Device name changes	Restricted
Wallpaper changes	Optional: restrict for shared devices
Bluetooth changes	Restricted if not needed
MDM profile removal	Blocked

Suggested Mosyle Profile Structure

Student settings should be split into multiple Mosyle profiles instead of one large profile. This makes management, troubleshooting, and grade-level customization much easier.

Profile Name	Purpose
Students - Restrictions	AirDrop, Siri, App Store, iCloud, Game Center, account changes, device changes
Students - Security	Passcode, auto-lock, FileVault, firewall, Gatekeeper, profile removal protection
Students - Wi-Fi	Student Wi-Fi, certificates, auto-join, network restrictions
Students - Apps	Required apps, blocked apps, approved learning tools, app removal restrictions
Students - Web Filtering	CIPA-aligned filtering, malware protection, category restrictions, bypass prevention
Students - Testing Mode	Assessment restrictions, app lock, browser lock, testing-specific controls

Recommended Final Student Standard

Category	Recommended Setting
USB storage	Blocked
Siri	Disabled
Siri while locked	Disabled
AirDrop	Disabled
Personal Apple ID	Blocked
iCloud Photos	Disabled
iCloud Keychain	Disabled
App installs	Mosyle-managed only
Removing managed apps	Blocked
Game Center	Disabled
Messages	Disabled unless required
FaceTime	Disabled unless required
Camera	Allowed if needed for instruction

Category	Recommended Setting
Microphone	Allowed if needed for instruction
Screen recording	Restricted unless approved
VPN apps	Blocked unless school-managed
DNS / proxy changes	Restricted
Private browsing	Disabled where possible
Web filtering	Required
SafeSearch	Enforced
YouTube Restricted Mode	Enforced where applicable
Password / Passcode	Required based on grade/device type
Auto-lock	Required
Admin rights	Not allowed
MDM profile removal	Blocked

Recommended Grade-Level Approach

Not all students need the same level of restriction. The school may want to separate student profiles by grade band.

Grade Level	Recommended Approach
K–2	Most restrictive; only required apps; very limited settings access
3–5	Highly restricted; allow only approved learning apps and websites
6–8	Restricted with some flexibility for projects, research, and classroom tools
9–12	Controlled but more flexible; still block bypass tools, unmanaged apps, and risky content

Recommended Exception Process

Student exceptions should be limited and documented. Exceptions should normally be tied to a class, grade level, accessibility requirement, testing requirement, or approved instructional activity.

Example Exceptions

- STEM class needs Bluetooth or USB access for robotics
- Media class needs camera and microphone access
- Testing group needs a special locked-down testing profile
- Student requires Dictation or accessibility tools
- High school course requires access to specific approved websites

Exception Documentation Should Include

- Student name or group
- Grade level
- Device serial number or assigned device group
- Requested exception
- Instructional or accessibility reason
- Approving staff member
- Expiration or review date

Revision #1
Created 2026-05-21 18:39:06 UTC by joliveira
Updated 2026-05-21 18:40:24 UTC by joliveira