Best Practices

- Recommended Standard Teacher MDM Profile
- Recommended Standard Student MDM Profile

Recommended Standard Teacher MDM Profile

This guide provides a recommended baseline configuration for **teacher and staff Apple devices** managed through **Mosyle MDM**. The goal is to create a balanced standard that protects school data, reduces classroom distractions, and keeps devices consistent without overly limiting teachers from doing their work.

> **Recommended Profile Name:**
> `Staff / Teacher – Standard Security & Classroom Use`

Purpose

This profile should be applied to school-owned teacher and staff devices such as MacBooks, iPads, and other Apple devices assigned to employees. This profile should be less restrictive than a student device profile, but more controlled than a personal unmanaged device.

- Protect school data
- Reduce security risks
- Limit classroom distractions
- Keep device settings consistent
- Allow teachers to use approved instructional tools

Recommended Mosyle Profile Naming Examples

```
Staff - macOS - Teacher Baseline
Staff - iPadOS - Teacher Baseline
Staff - Standard Restrictions
Staff - Security Baseline
Staff - Web Filtering
```

Recommended Baseline Settings

1. USB Storage / External Drives

> **Recommendation:** Restrict USB storage where possible, or allow only by documented exception.

Setting	Recommendation
USB storage access	Allow only if needed
Unknown USB accessories	Restrict when device is locked
External drive writing	Restrict where possible
External drive reading	Allow only for approved workflows

USB drives are one of the easiest ways for school data to leave a device. They can also introduce malware or create data-loss concerns. Teachers may have legitimate reasons to use external storage, but the standard should be to use approved cloud storage instead whenever possible.

Suggested policy language:

> *Teachers should avoid using personal USB drives for school data. Approved school cloud storage should be used whenever possible to reduce the risk of data loss, malware, or unauthorized transfer of sensitive information.*

2. Siri

> **Recommendation:** Disable Siri on school-owned teacher devices unless there is an accessibility need.

Setting	Recommendation
Siri	Disabled
Siri while locked	Disabled
Dictation	Allowed only if needed for accessibility

Siri is usually not required for classroom instruction or staff productivity. Disabling Siri reduces privacy concerns, prevents accidental voice activation, and removes unnecessary lock-screen access.

3. AirDrop

> **Recommendation:** Disable AirDrop by default. Allow only by exception for approved instructional use.

Setting	Recommendation
AirDrop	Disabled by default
AirDrop from Everyone	Not allowed
Password sharing through AirDrop	Disabled

AirDrop can be useful, but in a school setting it can also be abused for distractions, inappropriate file sharing, or accidental exposure of sensitive information.

Possible exception groups:

- Art teachers
- Media teachers
- STEM teachers
- Yearbook staff
- Technology staff

4. Apple ID and iCloud

> **Recommendation:** Restrict personal Apple ID use on school-owned devices.

Setting	Recommendation
Personal Apple ID	Not allowed on school-owned devices
Managed Apple ID	Preferred
iCloud Drive	Disabled unless approved
iCloud Photos	Disabled
iCloud Keychain	Disabled

School-owned devices should not become tied to personal Apple IDs. This can create problems with Activation Lock, app ownership, data ownership, privacy, and long-term device support.

5. App Store and App Installation

> **Recommendation:** Apps should be deployed through Mosyle using Apple School Manager Apps and Books.

Setting	Recommendation
App Store	Restricted
User app installation	Disabled or limited
Managed apps	Required method
Removing managed apps	Disabled

6. Classroom Distraction Controls

Feature	Recommendation
Game Center	Disabled
Messages	Disabled unless approved

Feature	Recommendation
FaceTime	Disabled unless approved
Camera	Allowed
Microphone	Allowed
Screen Recording	Allowed for teachers

Teachers should have access to instructional tools such as the camera, microphone, screen recording, printing, and approved classroom applications. Consumer features that do not support instruction should be limited.

7. Privacy and Security

> **Recommendation:** Enforce security settings on all school-owned teacher devices.

Security Item	Recommendation
Password / Passcode	Required
Auto-lock	Required
FileVault on macOS	Enabled
Firewall on macOS	Enabled
Gatekeeper	Enabled
Local admin rights	Standard user preferred

8. Web Filtering and Content Protection

Teacher devices should still have web filtering enabled, but the teacher policy should be less restrictive than the student policy. Teachers may need access to broader educational content, research tools, media, and administrative websites.

Category	Recommendation
Adult content	Blocked
Malware / phishing	Blocked

Category	Recommendation
Risky categories	Blocked
YouTube	Allowed with staff-level filtering
Social media	Allow or limit based on school policy

Suggested Mosyle Profile Structure

Instead of placing every setting into one large profile, it is better to split the configuration into smaller Mosyle profiles. This makes troubleshooting easier and allows IT to update one area without affecting everything else.

Recommended Profiles

Profile Name	Purpose
Staff - Restrictions	AirDrop, Siri, Game Center, App Store, iCloud, sharing controls
Staff - Security	Password, FileVault, firewall, auto-lock, Gatekeeper
Staff - Wi-Fi	School Wi-Fi, certificates, auto-join settings
Staff - Apps	Required apps, classroom tools, security agents, print clients
Staff - Web Filtering	Staff-level filtering policy, malware protection, content protection

Recommended Final Standard

Category	Recommended Setting
USB storage	Restricted / exception only
Siri	Disabled
Siri while locked	Disabled
AirDrop	Disabled

Category	Recommended Setting
Personal Apple ID	Not allowed
iCloud Photos	Disabled
iCloud Keychain	Disabled
App installs	Mosyle-managed only
Game Center	Disabled
Camera	Allowed
Microphone	Allowed
Screen Recording	Allowed for teachers
Printing	Allowed
FileVault	Enabled
Firewall	Enabled
Password / Passcode	Required
Auto-lock	Required
Web filtering	Enabled
Admin rights	Standard user preferred

Recommended Exception Process

Some teachers may need exceptions based on their role or instructional workflow. Exceptions should be intentional, approved, and documented.

Example Exceptions

- Art teacher needs AirDrop for media workflow
- STEM teacher needs USB storage for robotics equipment
- Music teacher needs external audio devices
- Media teacher needs camera, microphone, and screen recording access

- Administrator needs broader website access

Exception Documentation Should Include

- User or group name
- Device serial number
- Requested exception
- Business or instructional reason
- Approval person
- Review date

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