Apple in Education Data and Privacy Overview for Schools

Contents

For 40 years, Apple technology has helped to expand how teachers teach and students learn, with access to powerful tools and apps that enable engaging learning experiences and unleash the creative potential in every student. We know how important security and privacy are to protect the data that students create, store, and access throughout the learning experience.

Security and privacy are fundamental to the design of all Apple hardware, software, and services. We take an integrated approach to ensure that every aspect of the experience has security and privacy built in. This approach considers the privacy and security of all users, including those within an education setting such as teachers, faculty, staff, and students.

We have also created features and services that are designed specifically for education, including Apple School Manager, Managed Apple IDs, and Shared iPad. These capabilities are built with the same integrated approach and with additional consideration for the specific security and privacy needs of students and institutions.

This overview covers how Managed Apple IDs and our related education features and services handle student data and privacy. You can use this overview to communicate to parents about how their students' data is secured by Apple.

Apple's Commitment to Student Privacy

Apple will never track, share, or sell student information for advertising or marketing purposes. We don't build profiles of students based on their email content or web browsing habits. We also don't collect, use, or disclose personal student information other than to provide educational services. Apple will not sell personal student information or disclose student information for targeting of advertisements to students.

As a further demonstration of our commitment, Apple has created an Apple Privacy Policy along with the Apple School Manager Agreement to cover how we collect, use, disclose, transfer, and store user information. We have also signed the Student Privacy Pledge.

Apple School Manager and Managed Apple IDs

Apple provides services for schools and educational institutions of all sizes to easily deploy iPad and Mac. These services have been built with security and privacy in mind to ensure your institution's and students' data is protected before, during, and after your deployment.

Apple School Manager is a free web-based service that has everything IT administrators need to deploy iPad and Mac in schools. Apple School Manager lets you buy content, configure automatic device enrollment in your mobile device management (MDM) solution, create accounts for your students and staff, set up class rosters for the Schoolwork and Classroom apps, enable the Student Progress feature, and manage apps and books for teaching and learning.

A central capability of Apple School Manager is the ability to create institutionally controlled Managed Apple IDs. Managed Apple IDs give students access to iCloud Drive, Photo Library, Backup, Schoolwork, and Shared iPad, while maintaining the control schools need. Managed Apple IDs are designed for educational purposes only.

To ensure that schools providing devices to students are only enabling use for the purposes of education, we've disabled certain features and functions of Managed Apple IDs. Students cannot make App Store, Apple Books, Apple TV, Apple Podcasts, and Apple Music purchases. Also, Apple Pay, Find My, iCloud Mail, HomeKit, and iCloud Keychain are all disabled. FaceTime and Messages are also disabled by default, but can be enabled by the school's IT administrator.

Apple School Manager lets you automatically create Managed Apple IDs for all students and staff in the following ways:

You can use federated authentication to connect Apple School Manager with your school's Microsoft Azure Active Directory (AD) so users will be able to sign in to Apple services with their Active Directory user name and password. Microsoft Azure AD is the Identity Provider (IdP), which contains the user names and passwords for the accounts you want to use with Apple School Manager. Federated authentication uses Security Assertion Markup Language (SAML) to connect Apple School Manager to Microsoft Azure AD. At no time is data written back to Azure AD.

You can also import only the necessary data from your Student Information System (SIS) or CSV files exported from your school's directory service. Each user account is created with read-only information from the source. Additional information, such as the Managed Apple ID identifier and associated password, is added to the account information in Apple School Manager. At no time is data written back to your SIS.

Managed Apple IDs can also be created manually within Apple School Manager.

Each user account may have the following information associated with it, which can be viewed in the account list or when an account is selected:

- An alphanumeric ID unique to that account
- First, middle, and last name
- Grade level, if provided
- Enrolled classes
- Email address, if provided
- Role
- Location
- Source
- Date created
- Date modified

Because Managed Apple IDs are created and assigned by your institution, you can easily reset passwords, inspect accounts, and define roles for everyone in the district. Anytime an account is inspected by an IT administrator or subject to a password reset, Apple School Manager logs the action so a record of the activity is retained.

Managed Apple IDs also support a range of passcode options from simple four-digit numeric to complex alphanumeric. Apple School Manager creates temporary passwords for accounts when they are initially imported or created. These temporary passwords are for users of the accounts to sign in with their Managed Apple ID for the first time, at which point the user must change their password. Apple School Manager never shows the student's chosen password once it has been changed from the temporary password. A student can sign in on a device not managed by the institution to access their school work; for example, a device at home. To do so, they can sign in with their Managed Apple ID, password, and a six-digit verification code provided by the IT administrator through Apple School Manager. This additional verification code expires after one year.

If a Managed Apple ID is created through federated authentication, the password and all related settings, such as password options, multi-factor authentication, password resets, etc., are managed exclusively in Microsoft Azure Active Directory.

When an institution deletes a Managed Apple ID, all information associated with that account will be deleted from Apple's servers within a maximum of 30 days. And when a school wishes to cease to use Apple School Manager, all student data will be deleted within a maximum of 180 days.

Schoolwork

The Schoolwork app helps teachers share instructional materials and better understand student progress within the apps and books they use with their students. Schoolwork uses student and class roster information that IT administrators set up in Apple School Manager.

A school can optionally enable the Student Progress feature in Apple School Manager, so that app developers can privately and securely share student progress data with teachers on activities, like reading a chapter in a book, completing a set of math equations, or taking a quiz, assigned in school managed environments. This data allows teachers as well as students to better understand learning progress on assigned activities, and enables teachers to provide extension activities or extra help based on student needs.

Progress data shared with teachers depends on the type of data generated by the progress-reporting app, which is defined by the app developer and may include time spent on the activity based on start and end times, percentage completed, quiz scores, hints used, numeric values such as word count and points earned, or binary values such as Yes/No and True/False. At a minimum, every activity that supports progress reporting sends time spent data.

The Student Progress feature was designed to protect student privacy. When a school enables the Student Progress feature in Apple School Manager, student progress data is shared only for activities a teacher specifically assigns as part of an assignment using Schoolwork, and only when students are using their Managed Apple ID, created for them by their school, on their device. Student progress on any activities that were not assigned will not be shared or displayed. For example, if a teacher assigns students to read the Prologue of *Romeo and Juliet* in Apple Books, and a student also reads *The Great Gatsby*, the student and the teacher will see progress data only on the Prologue because that was the assigned reading. To ensure transparency when progress reporting is active, students will see a notification indicating that their progress is being reported.

In addition to the Student Progress feature, your school's IT administrator can enable the Improving Schoolwork feature in Apple School Manager. If enabled, Apple can process non-personally identifying Schoolwork data using techniques such as machine learning to improve the app. For example, Apple may process Schoolwork data to understand trends in usage, customize user experience, and develop new education features for the app. To ensure transparency, students and teachers will see an onscreen notification the first time they access Schoolwork using their Managed Apple ID after Improving Schoolwork is enabled.

Classroom

The Classroom app enables teachers to manage student iPad devices in the classroom, helping them guide students through a lesson by opening apps and links for them. Teachers can easily send and receive documents with everyone in the class and keep an eye on the students' work by viewing their screen.

With Classroom, student iPad devices can be managed only in class and no data is stored after a class session ends. The teacher and students need to be in close proximity, signed on to the same Wi-Fi network, and in an active class session. The teacher cannot manage or view student devices outside of class. To ensure transparency when Screen View is active for a student's screen in class, a notification at the top of their screen indicates that the screen is being viewed. Schools can also choose to disable Screen View if they prefer that teachers not view student screens.

Managed Apple IDs and Shared iPad

In the cases where students will be sharing an iPad, Apple provides the ability for students to log in with a Managed Apple ID to quickly access and work with their own apps, content, and settings. This enables multiple students to use the same iPad, while ensuring a personal learning experience.

When a student signs in to Shared iPad, the Managed Apple ID is automatically authenticated with Apple's identity servers. If the student has not used the device before, a new home directory and keychain are provisioned for the user. After the student's local account has been created and unlocked, the device will automatically sign in to iCloud. Next, the student's settings are restored and their documents and data are synced from iCloud.

While the student session is active and the device remains online, documents and data are stored in iCloud as they are created or modified. In addition, a background syncing mechanism ensures that changes are saved to iCloud after the student signs out.

iCloud and Data Security

As students create documents, interact with lessons, and engage in classroom activities, it's important that they can safely store their data and also ensure it's protected at all times—both on the device and in iCloud.

With iCloud, users can have their documents, contacts, notes, bookmarks, calendar events, and reminders automatically saved so they can access the information across iOS and Mac and at iCloud.com on a Mac or PC. Managed Apple IDs are enabled for these services by default, with access to 200GB of free iCloud storage. If the user signs in to iCloud, apps are granted access to iCloud Drive. Users may control each app's access under iCloud in Settings.

iCloud is built with industry-standard security practices and employs strict policies to protect data. iCloud secures the user's information by encrypting it when it's in transit, storing it in an encrypted format, and securing their encryption keys in Apple data centers. When processing data stored in third-party data centers, such as Amazon Web Services, encryption keys are accessed only by Apple software running on secure servers, and only while conducting the necessary processing. For additional privacy and security, many Apple services use end-to-end encryption, which means that only the user can access their information, and only on trusted devices where the user is signed in with their Apple ID.

Apple has received ISO 27001 and ISO 27018 certifications for implementing an Information Security Management System with measures for protecting personally identifiable information (PII) in public cloud environments. Apple's compliance with the ISO standard was certified by the British Standards Institution (BSI). Learn more about Security Certifications at the Security Certifications for Apple Internet Service and more about iCloud security at the iCloud Security Overview.

CloudKit and Third-Party Apps

Third-party apps are an essential element of a modern learning environment. In order to enable students to have the same seamless experience of storing and retrieving their data in third-party apps, we've created CloudKit—a framework third-party developers can use to store and sync data to iCloud.

With an app that uses CloudKit, students are automatically signed in with their Managed Apple ID, which means they don't have to create a new account or provide other personal information. They will always have access to their latest information in the app without having to remember new user names or passwords. Developers don't have access to the student's Managed Apple ID, just a unique identifier.

Whether the developer is using CloudKit or not, it's important to be aware that third-party apps may be collecting data about the student. It is your school's responsibility to ensure compliance with all applicable laws when using third-party apps. Your school should review the terms, policies, and practices of third-party apps to understand what data they may collect from students, how such data is being used, and whether parental consent is required.

On the App Store, Apple requires app developers to agree to specific guidelines that are designed to protect user privacy and security. We have placed additional requirements on all developers adopting our framework for student progress reporting with Schoolwork, called ClassKit. In addition to our standard requirements for publishing an app on the App Store, we require that developers adopt ClassKit only if their use of ClassKit is designed to provide educational services. They must not serve behavioral advertising in the app, and they must provide a suitable privacy policy of all of their data use.

If we become aware of an app that violates our guidelines, the developer must address the issue or be removed from the App Store.

Location Services and Lost Mode

As students use apps and services on their device, they may be prompted to enable Location Services depending on the specific app or activity within the app. Apple provides users granular control over how location data is managed and shared with apps and cloud services. Location Services are turned off by default, but can be turned on by the student if allowed by the school.

Apple's built-in location-based apps, such as Maps, Weather, or Camera, need to request permission to gather and use data that indicates location. The location data collected by Apple is collected in a form that does not personally identify the student. Other apps made available by the school also need to request permission to access location data. Students, like all our customers, can approve and revoke access for each app that asks to use the service.

Access can be set to never allowed, allowed when in use, or always, depending on the app's requested location use. Users may choose not to allow this access, and may change their choice at any time in Settings. Also, if apps granted access to location data at any time make use of this permission while in background mode, users are reminded of their approval and may change an app's access. When an app is using Location Services, an arrow icon appears in the menu bar.

A user's location is not routinely available to the school through Apple's features and services. However, Location Services can be used to help a school recover a lost or stolen device. On a school device, an MDM administrator can remotely enable Lost Mode. When Lost Mode is enabled, the current user is logged out and the device cannot be unlocked. The screen displays a message that the administrator can customize, such as displaying a phone number to call if the device is found. When the device is put into Lost Mode, the administrator can request the device to send its current location back to the MDM server. When an administrator turns off Lost Mode for a device, the device location will be sent and the user informed of this action.

International Data Transfer

Apple works with schools around the world to enable teachers and classrooms with the best tools for learning. To support the use of Apple services, we also work with governing bodies to ensure data processing requirements are met.

With Apple School Manager, Managed Apple IDs, and iCloud, personal information may be stored in locations outside the country of origin. Wherever the data is stored, it will be subject to the same strict data storage standards and requirements.

If required by law, Apple will ensure that any international data transfer is done only to a country that ensures an adequate level of protection, has provided appropriate safeguards as set forth in applicable law (e.g. the EU's standard contractual clauses), or is subject to a derogation. The standard contractual clauses are referenced in the Apple School Manager Agreement.

Privacy Overview for Parents

Transparency is important when it comes to understanding how a student's information is being used. To help address any questions that parents or guardians may have, we created a privacy overview for parents. We encourage you to distribute it to your school community to explain how student information is collected, used, and stored when schools use education services and apps from Apple.

Additional Resources

At Apple, your school's and your students' trust mean everything to us. That's why we respect students' privacy and protect it with strong encryption, plus strict policies that govern how all data is handled.

Access the following resources for more information, or if you have questions about privacy, you can contact us directly at apple.com/privacy/contact.

- About Privacy and Security for Apple Products in Education: support.apple.com/kb/HT208525
- Privacy Overview for Parents: apple.com/education/docs/Privacy_Overview_for_Parents.pdf
- Apple Education, IT & Deployment: apple.com/education/it
- Apple School Manager Agreement: apple.com/legal/education/apple-school-manager
- Apple School Manager User Guide: support.apple.com/guide/apple-school-manager
- Education Deployment Guide: help.apple.com/deployment/education
- iOS Security Guide: apple.com/business/docs/iOS_Security_Guide.pdf
- Apple's Commitment to Your Privacy: apple.com/privacy