



Apple in Education

Data and Privacy Overview for Schools

Education has always been part of Apple's DNA. We believe technology has the power to transform every classroom and engage every student. Our products are designed to expand how teachers teach and students learn with access to powerful apps and engaging content on the devices they love to use. We also know how important security and privacy is to protect the data 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 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 and students' data is protected before, during and after your deployment.

Apple School Manager is a free web-based service that has everything technology managers need to deploy iPad and Mac in schools. Apple School Manager lets you buy content, configure automatic device enrolment in your mobile device management (MDM) solution, create accounts for your students and staff, and set up iTunes U courses.

A central capability of Apple School Manager is the ability to create institutionally controlled Managed Apple IDs. Managed Apple IDs are a new kind of Apple ID that give students access to iCloud, iTunes U, 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 purchase anything on the App Store, iBooks Store or the iTunes Store. Also, Apple Pay, Find My Friends, Find My iPhone, iCloud Mail, HomeKit, and iCloud Keychain are all disabled. FaceTime and iMessage are also disabled by default, but can be enabled by an administrator.

Apple School Manager lets you automatically create Managed Apple IDs for all students and staff by importing 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.

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 administrator or 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 administrator through Apple School Manager. This additional verification code expires after one year.

An Apple School Manager administrator can release a Managed Apple ID account making it accessible by the student, instructor, staff, or manager for approximately 180 days, after which all data associated with that account will be permanently deleted. Should an institution request the immediate deletion of a Managed Apple ID, the account will no longer be accessible and all information associated with that ID will be permanently deleted within 40 days.

Managed Apple IDs and Shared iPad

In the cases where students will be sharing an iPad, Apple provides the ability for students to login 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](https://www.icloud.com) on a Mac or PC. If the user signs in to iCloud, apps are granted access by default to iCloud Drive. Users may control each app's access under iCloud in Settings. Managed Apple IDs are enabled for the above services by default.

iCloud is built with industry-standard security practices and employs strict policies to protect data. iCloud secures user data by encrypting it when it's sent over the Internet, storing it in an encrypted format when kept on the server, and using secure tokens for authentication. This means that student data is protected from unauthorized access both while it is being transmitted to devices and when it is stored in iCloud. iCloud uses a minimum of 128-bit AES encryption—the same level of security employed by major financial institutions—and never provides encryption keys to any third parties. Apple retains the encryption keys in our own data centres. iCloud also stores student passwords and credentials in such a way that Apple cannot read or access them.

For more information about iCloud security and privacy, visit <https://support.apple.com/en-ca/HT202303>.

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 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 Apple ID, just a unique identifier.

Regardless of if 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. When 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 will likely be prompted to enable location services depending on the specific app or activity within the app. Apple has provided users granular control over how their location data is managed and shared with apps and cloud services.

Location Services lets location-based apps, such as Maps, Weather, and Camera, gather and use data that indicates location. The location data collected by Apple isn't collected in a form that personally identifies your student. Location Services is turned off by default, but can be turned on using a single switch in Settings. Students can approve access on a per app basis for each app that asks to use the service.

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

Location services are also used to help your school recover a lost or stolen device. On a supervised device with iOS 9.3 or later, 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 can be customized by the administrator, 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 also be sent and the user informed of this action.

Diagnostic Data

If you and your students would like to help improve Apple products and services, you can opt in to our Diagnostic and Usage program and send non-identifiable information about your device and applications to Apple.

Explicit consent is required to do this. Users can view the data on their device or stop sending data at any time through Settings, or for Shared iPad deployments your school can disable the submission of Diagnostic and Usage data through a restriction.

iOS also features advanced diagnostic capabilities that may be useful in debugging or troubleshooting device problems. These advanced diagnostic capabilities do not send any data to Apple without additional tools and explicit consent.

International Data Transfer

Apple works with schools around the world to enable teachers and classrooms with the best tools for learning.

With Apple School Manager, Managed Apple IDs, iTunes U and iCloud, personal data 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.

Apple ensures that Personal Data transferred from the European Economic Area or Switzerland to the United States of America is governed either by any operative Safe Harbor program, or its successor, to which Apple Inc. is certified, or Model Contractual Clauses/Swiss Transborder Data Flow Agreement which are appended to the Apple School Manager Agreement.

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 strict policies that govern how all data is handled.

Access the following additional resources for more information, or if you have questions about privacy, you can always contact us directly at <http://www.apple.com/ca/privacy/contact/>.

Apple's Commitment to Your Privacy: <http://www.apple.com/ca/privacy/>

Apple Education: IT & Deployment www.apple.com/ca/education/it/

Apple School Manager Agreement: www.apple.com/legal/education/apple-school-manager/

Apple School Manager Help: help.apple.com/schoolmanager/

Education Deployment Guide: help.apple.com/deployment/education/

iOS Security Guide: www.apple.com/ca/business/docs/iOS_Security_Guide.pdf



© 2016 Apple Inc. All rights reserved. Apple, the Apple logo, Apple Pay, FaceTime, iMessage, iPad, iTunes U, Mac, Siri, Spotlight, and Touch ID are trademarks of Apple Inc., registered in the U.S. and other countries. HomeKit is a trademark of Apple Inc. iCloud and iTunes Store are service marks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. May 2016