Apple Education
Parent Guide to Privacy

This guide is designed to help parents and guardians understand how Apple helps protect the privacy of your student's information. Our goal is to provide the best tools for learning, while making sure our technology works in ways that protect your student's privacy and keep their data safe. Privacy and security are fundamental to the design of Apple's hardware, software, and services, and we have the following policies regarding student information:

- We don't sell student information, and we never share it with other companies for marketing or advertising purposes.
- We don't build profiles of students based on email content or web browsing habits.
- We don't collect, use, or disclose personal student information other than to provide relevant educational services.

Whether your school provides an iPad or a Mac, or your student brings their own device to school, this guide provides privacy details about the following categories related to the student experience:

- **Student accounts**—an ID from Apple that gives your student access to services and other learning materials.
- **Student data**—the information stored about your student, and the information your student produces by creating digital work.
- **Device management**—how schools set up and manage iPad and Mac to ensure a productive learning environment.
- **Digital citizenship**—the best practices for using technology at school and at home.

Student Accounts

iPad and Mac are like your student's locker, desk, and lab bench all in one—a place where their materials and schoolwork are all instantly accessible. For example, your student may be reading and taking notes on their iPad or Mac, or creating multimedia projects to document a science experiment. To save work or access other Apple resources, your student needs an account with Apple. There are two types of accounts—a consumer account simply called an Apple ID, and accounts designed for schools called Managed Apple IDs. This guide will focus on Managed Apple IDs.

Managed Apple IDs

Unlike consumer Apple IDs, Managed Apple IDs are owned and controlled by the school or district and are designed to meet school needs, including limitations on purchasing and communications. A Managed Apple ID allows your student to sign in to their iPad or Mac and access Apple services such as iCloud, Apple's cloud service, and iTunes U. With Managed Apple IDs, some Apple services such as Apple Pay, HomeKit, and Find My iPhone are disabled. Managed Apple IDs also do not support student purchasing on the App Store, the iTunes Store, or Apple Music.

Schools can create Managed Apple IDs for students while maintaining privacy and security. These IDs are built with two-factor authentication, a widely adopted security practice. To maintain student privacy, Managed Apple IDs use a limited amount of student information. For example, the data associated with a Managed Apple ID at account creation is limited to the student's name, grade level, class, and student ID. (The school may optionally provide your student's email address or photo.) Other data that the school may have about the student remains stored separately in the school's Student Information System (SIS).

Managed Apple IDs can also be used for schoolwork with a personally owned iPad or Mac. For schoolwork at home, your student may sign in to iCloud with their Managed Apple ID, then use a home-use password issued by the school for two-factor authentication purposes. Even at home, when your student uses a Managed Apple ID on a personally owned device, the school may have restricted the use of features such as FaceTime or iMessage. Note: iCloud documents created by students when they are signed in with their Managed Apple ID are also subject to audit as described below.

Managed Apple IDs are for use in a school environment. Outside of school, students 13 and older, depending on the jurisdiction, can access Apple's commercial offerings by creating a personal Apple ID. Students 13 and younger can have an Apple ID as part of a family using Family Sharing.

If a school considers it appropriate for students to log in to a school-managed device with a personal Apple ID, such use of a personal Apple ID will become subject to Apple's privacy policy and additional terms of service. The school should therefore ensure that use of a personal Apple ID is acceptable under applicable domestic laws and school policies.

Auditing Managed Apple IDs

Managed Apple IDs support the ability to conduct an audit of the student's account at the school's discretion. This feature maintains a strict protocol that logs all audits. It works by granting an administrator, a manager, or a teacher auditing privileges in Apple School Manager, Apple's IT portal. When an account is inspected by the school, the action is recorded and time-stamped with the auditor's credentials. During the audit period, the auditor can read and modify the user's content stored in iCloud or apps that store data in iCloud. Auditing permissions expire after seven days. If necessary, parents may coordinate with their school administration to audit their student's account.

Communications: Text messages, email, voice/video chat

Managed Apple IDs cannot be used for email. Apple's messaging and video chat services, iMessage and FaceTime, are disabled by default; schools can choose to enable these two features, which would then be subject to the terms associated with those features. To understand email and electronic communications policies at your school, ask your school administrator for a copy of the school's policies.

Student Data

Today's students can take notes, sketch, design, code, animate, record, publish, and complete assignments on iPad and Mac. To help ensure that your student's information is kept private and secure along the way, Apple handles data using a "data minimization" approach. The following paragraphs give examples of how student data may be handled regarding location, security, ownership, commercial activity, and compliance.

Location information

Location Services allows location-based apps and websites to use location data. For example, a student might need to map bird species around the world in a science class, or while on a field trip. When setting up their device for the first time, students can enable Location Services in Setup Assistant. Your school's mobile device management (MDM) solution can hide this choice for school-owned devices, making Location Services disabled by default. Apple provides granular control over how location data is used on a per-app basis, and these settings can be set by the student to *never allowed*, *allowed when in use*, or *always*.

As students use their device, they will likely be prompted to enable Location Services by various apps. If students have allowed an app to always access Location Services, they may be reminded of their choice occasionally and can change their mind at any time.

Security on the device, and in the cloud

As your student creates documents, works with content, and engages in classroom activities, it's essential that they can safely store their work knowing that their privacy is protected. Built with security and privacy in mind, our services ensure that both student and school data are protected before, during, and after the devices are handed to students.

When thinking about data, you'll find it's helpful to break it up into two areas: data on the device, and data stored in the cloud. Some schools may use Shared iPad, a feature in iOS that provides a personal learning experience on iPad devices that rotate among different students throughout the day. With Shared iPad, each student saves their own work and settings to iCloud with their Managed Apple ID before they leave class. Their work is automatically saved to iCloud in a way that protects it from access by other students who share the iPad.

Student work can be stored safely on iPad or Mac because data is encrypted on the device. Encryption is enabled automatically on iPad, and can be enabled with FileVault on Mac. This means that without the student's password, the data on their device cannot be accessed.

iCloud, Apple's cloud service, requires a secure network protocol called HTTPS whenever data moves from place to place. iCloud is built with industry-standard security practices and employs strict policies to protect data. On iPad and Mac, an encrypted connection is also required whenever it connects to a service or the Internet.

iCloud secures user data by encrypting it when it's sent over the Internet, storing it in an encrypted format when it's 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 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 centers. 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-us/HT202303.

Data ownership

Apple does not own student data on devices or in the cloud. While your school or district may control how and when students access services and content on their devices, student work remains their own. You can review the details of your school's data practice policies for more information.

Student Privacy Pledge

The Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA) introduced a Student Privacy Pledge to safeguard student privacy, and Apple has signed the Student Privacy Pledge. To learn more, see the Student Privacy Pledge.

Global compliance

Apple works with schools around the world to provide the best technology for learning and has received the ISO 27001 data certification. 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.

Device Management

To support the learning environment, your school will likely set up and manage your student's iPad or Mac, and the apps and books it contains. Device management software solutions help schools ensure that policies and settings are established on school-owned devices, as well as on student-owned devices brought to school. In this section, we'll review common tools for managing devices that help keep your student's information safe and secure. Understanding who owns the iPad or Mac used by your student is also important, because this can determine which features are managed by the school.

There are three basic ownership scenarios in schools:

- **One-to-one deployment**: The school purchases an iPad or a Mac and provides it to each student. This type of deployment may be for a particular grade level, a department, or an entire district or university.
- **Shared deployment**: The school purchases and provides a set of iPad or Mac devices that rotate among students.
- **Bring-your-own-device deployment** (BYOD): You purchase an iPad or a Mac for your student to use at their school or university.

Managing devices

Your student's device may be managed by a mobile device management (MDM) solution—a third-party service that provides software to manage device settings and resources. With MDM, schools can set up devices for student use by installing apps, books, and other educational content provided by the school. A school administrator sets the policies for which features can be enabled or disabled on iPad and Mac, in apps, and on the school network. MDM software is typically required to manage devices owned by the school, and it is optional in a BYOD scenario.

If your school owns your student's device, MDM settings for iPad and Mac can be configured so the settings cannot be removed. This is the standard practice in most one-to-one and shared-device deployments. And for schools using the Shared iPad feature, MDM is required.

If your student brings their own device to school, they must opt in to the school's management software. In this case, since the school does not own the device, MDM device settings can be removed by a student or parent at any time.

IT administrators have only limited access to student data and location information on managed Apple devices. MDM software cannot see everything on a student's device; it can interact with a device only through notifications that are used to configure settings or install apps. This helps prevent monitoring or tracking of student devices. If a device is lost or stolen, an IT administrator can remotely look for that device with a feature called Managed Lost Mode, but only after a message is sent to the device notifying the user that it is lost and its location is being accessed. When the administrator turns off Managed Lost Mode, the user is informed both through a message on the Lock screen and an alert on the Home screen.

Apple School Manager and student information

Apple School Manager, Apple's administrative portal for IT, is built with student privacy in mind. For example, Apple School Manager imports only the data required for basic account and class roster setup; other student information that the school may have is not imported. Your school may use Apple School Manager to create Managed Apple IDs for use by students, teachers, and other staff.

Configuring devices

Your school decides how to configure iPad and Mac to meet the requirements of a particular grade level or curriculum plan. The setup of apps and content is accomplished by sending a file to the device that tells it which settings, features, and apps to use. This file, called a configuration profile, is managed by the school. If the school does not use MDM, school administrators can provide links to download configuration profiles via email, or install profiles manually on devices using Apple Configurator, a tool available on Mac.

For one-to-one scenarios, it is most common for schools to use MDM to set up and manage devices. Students will typically receive devices on the first day of school with their own Managed Apple ID. (For more on Managed Apple IDs and MDM, see the Student Accounts section on page 1.)

In shared deployments, devices may be set up in a general way, with a standard set of apps and learning materials. The most generalized shared deployment may not require a student to log in with an Apple ID. With iOS 9 (or later) software, the Shared iPad feature allows iPad to be personalized for each student. To access this multiuser mode, your student will use a Managed Apple ID, created by the school so students can save their own work and settings each time they use an iPad in class. With Shared iPad, student data is securely stored on the device and in iCloud, so each student's data is protected.

Nonmanaged devices

If your student is using their own iPad or Mac at school (BYOD), their device is not necessarily managed by the school. Some schools require that students opt in to the school-provided management software, even if the device is personally owned. Different schools will have different policies, so check with your school administrator on how devices are managed in your BYOD program.

Classroom app

Classroom is an iPad app from Apple that helps teachers guide learning with iPad in the classroom. The app lets teachers launch specific apps on every student iPad in the class, share a website, create activity groups, and see students' screens using Screen View. Teachers can also share a student's screen with the class using AirPlay and Apple TV. To help students focus, teachers can lock devices to a single app or temporarily lock the screens of all devices in the classroom.

While the Classroom app is designed to be a great tool for teachers, it is also designed to ensure best practices for transparency and student privacy. This means that student iPad devices can be managed only in class; the teacher cannot manage or view student devices outside the classroom. 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 it is being viewed. Schools can also choose to disable Screen View if they prefer that teachers not view student screens.

Digital Citizenship

Using technology in safe and responsible ways is referred to as digital citizenship. These practices include guidance on Internet safety, communications, cyberbullying, information literacy, creative credit, copyright, and more. Because learning in schools is so different now than it was just a few years ago, it is important for schools to adopt these best practices; all students, teachers, staff, and the school community should receive digital citizenship training.

Many resources are available to help students become good digital citizens and to guide schools and parents. Common Sense Media has materials for schools and their communities. Parents and their students should also review their school's technology policy regarding acceptable use, email, storing and charging devices, accessing content and apps, and more.

Digital citizenship resources

Digital citizenship on iTunes: www.itunes.com/digitalcitizenship

A Parents' Guide to Student Data Privacy from Future Privacy Forum: https://ferpasherpa.org/parents/a-parents-guide-to-student-data-privacy/

Common Sense Media

- Digital citizenship: https://www.commonsensemedia.org/educators/digital-citizenship
- Family guide: https://www.commonsensemedia.org/guide/essentialbooks
- Apps guide: https://www.commonsensemedia.org/guide/best-first-kids-apps

Resources

For more information on how Apple protects the security and privacy of students, access the resources below. If you have questions about privacy, you can contact us directly at www.apple.com/privacy/contact.

- Apple's commitment to your privacy: www.apple.com/privacy
- Data and privacy overview for schools: http://images.apple.com/education/docs/Education_Privacy_Schools_May16.pdf
- Apple School Manager help: https://help.apple.com/schoolmanager
- iCloud security and privacy: https://support.apple.com/en-us/HT202303
- Parental controls on Apple devices: https://support.apple.com/en-us/HT201304
- iTunes U security and privacy: https://support.apple.com/en-us/HT204918