Apple en la educación
Resumen de la privacidad de los datos para centros educativos

En Apple siempre hemos apostado por la educación. Creemos que la tecnología es capaz de transformar las aulas y motivar a todos los alumnos. Nuestros productos están pensados para ampliar las posibilidades de la enseñanza y el aprendizaje, ya que permiten a profesores y alumnos acceder a apps y contenidos increíbles en los dispositivos que más les gusta usar. También sabemos que es muy importante proteger los datos que los estudiantes crean, guardan y usan durante todo el proceso de aprendizaje.

La seguridad y la privacidad son una parte fundamental del diseño del hardware, el software y los servicios de Apple. Aplicamos un enfoque integrado para garantizar que cada aspecto de la experiencia sea 100 % confidencial y seguro. Este enfoque tiene en cuenta la privacidad y la seguridad de todos los usuarios, desde alumnos y profesores hasta el personal que trabaja en el centro.

También hemos creado prestaciones y servicios específicos para el sector educativo, como Apple School Manager, los ID de Apple Gestionados y los iPad Compartidos. Para ello aplicamos el mismo enfoque de seguridad y privacidad, y tenemos en cuenta, además, las necesidades específicas de los alumnos y los centros.

En este documento se resume cómo protegemos los datos y la privacidad de los estudiantes con los ID de Apple Gestionados y las prestaciones y los servicios dirigidos al sector educativo. Te servirá para explicar a los padres que Apple trata los datos de sus hijos con la más estricta confidencialidad.

El compromiso de Apple con la privacidad de los alumnos

Apple no rastrea, comparte ni vende bajo ningún concepto los datos de los estudiantes con fines publicitarios o de marketing. No creamos perfiles de estudiantes a partir del contenido de sus emails o las páginas web que suelen visitar. Tampoco recopilamos, usamos ni divulgamos los datos personales de los alumnos con otros fines que no sean ofrecer servicios educativos. Apple no venderá ni divulgará datos personales de los alumnos para ofrecer publicidad personalizada.

Como parte de nuestro compromiso, hemos creado una Política de Privacidad de Apple y el Acuerdo de Apple School Manager para dejar claro cómo recopilamos, usamos, divulgamos, transferimos y almacenamos la información del usuario. También hemos firmado el Student Privacy Pledge.

Apple School Manager y los ID de Apple Gestionados

Apple ofrece servicios que permiten implantar el iPad y el Mac en centros e instituciones educativas de cualquier tamaño. Son servicios totalmente seguros que garantizan que los datos de tu centro y tus alumnos están a buen recaudo antes, durante y después de la implantación.

Apple School Manager es un portal web gratuito que ofrece a los administradores todo lo necesario para implantar el iPad y el Mac en centros educativos. Te permite comprar contenidos, configurar la inscripción automática de dispositivos en tu solución MDM, crear cuentas para los alumnos y el personal del centro, y configurar cursos de iTunes U.

Una prestación clave de Apple School Manager es la capacidad de crear ID de Apple Gestionados cuya propiedad está en manos de los centros. Los ID de Apple Gestionados son un nuevo tipo de ID de Apple

que ofrece a los estudiantes acceso a iCloud, iTunes U y iPad Compartidos, al tiempo que proporciona a los centros el control que necesitan. Los ID de Apple Gestionados solo pueden usarse con fines didácticos.

Para garantizar que esto es así, hemos desactivado ciertas prestaciones y funciones en los ID de Apple Gestionados. Los alumnos no pueden comprar nada en el App Store, iBooks Store ni iTunes Store. Además, Apple Pay, Buscar a mis Amigos, Buscar mi iPhone, iCloud Mail, HomeKit y Llavero de iCloud están desactivados. FaceTime y iMessage también vienen desactivados por defecto, pero los puede activar un administrador.

Apple School Manager permite crear automáticamente ID de Apple para todos los alumnos y el personal del centro con solo importar los datos necesarios del Sistema de Información Gerencial (SIG) o archivos CSV exportados del servicio de directorio del centro. Cada cuenta se crea con información de solo lectura a partir de la fuente de origen. Aunque se añaden datos adicionales a la cuenta de Apple School Manager (como el identificador del ID del Apple Gestionado y la contraseña asociada), el sistema de información escolar no registra información procedente del centro en ningún momento.

Las cuentas pueden tener la siguiente información asociada, que puede verse en la lista o cada vez que se selecciona una:

- Un ID alfanumérico único para esa cuenta
- Nombre y apellidos
- Curso (si corresponde)
- Asignaturas
- Email (si corresponde)
- Cargo
- Ubicación
- Fuente
- Fecha de creación
- Fecha de modificación

Como cada centro crea los ID de Apple Gestionados y conserva su propiedad, es muy fácil restablecer contraseñas, inspeccionar cuentas y definir funciones para todos los usuarios. Cada vez que un administrador inspecciona una cuenta o restablece una contraseña, Apple School Manager lo registra en un historial para que quede constancia.

También se pueden usar distintas opciones de código, desde números sencillos de cuatro dígitos hasta códigos alfanuméricos complejos. Apple School Manager crea contraseñas temporales para las cuentas que se importan o se crean por primera vez. Estas contraseñas temporales sirven para que los usuarios puedan iniciar sesión con su ID de Apple Gestionado en ese momento, pero después deberán elegir otra. Apple School Manager nunca muestra la contraseña elegida por el alumno. Los estudiantes pueden iniciar sesión en un dispositivo que no esté gestionado por el centro para acceder a sus trabajos de clase, por ejemplo desde casa. Para ello, deben iniciar sesión con su ID de Apple Gestionado, su contraseña y un código de verificación de seis dígitos proporcionado por el administrador a través de Apple School Manager. Este código de verificación adicional caduca al cabo de un año.

Los administradores de Apple School Manager pueden habilitar una cuenta de ID de Apple Gestionado para un alumno, profesor, responsable o trabajador del centro durante unos 180 días. Transcurrido ese tiempo, todos los datos asociados a la cuenta se borrarán de forma permanente. Si un centro solicita que un ID de Apple Gestionado se borre de forma inmediata, la cuenta dejará de estar accesible y toda la información asociada a ella se eliminará en un plazo de 40 días.

ID de Apple Gestionados y iPad Compartidos

Si los alumnos van a compartir un iPad, Apple les permite iniciar sesión a cada uno de ellos con su ID de Apple Gestionado para acceder fácilmente a sus apps, contenidos y ajustes. De esta forma, varios alumnos pueden usar el mismo iPad y la experiencia de cada uno será totalmente personal.

Cuando un estudiante inicia sesión en un iPad Compartido, el ID de Apple Gestionado se verifica en los servidores de identidad de Apple. Si el estudiante no ha usado el dispositivo antes, se le proporciona un nuevo directorio de inicio y un llavero. Una vez que se ha creado y desbloqueado la cuenta local del estudiante, el dispositivo inicia sesión en iCloud de forma automática. A continuación, se restablecen los ajustes del estudiante y se sincronizan sus documentos y datos de iCloud.

Mientras la sesión siga activa y el dispositivo esté conectado, los documentos y los datos se irán guardando en iCloud a medida que el alumno los cree o los modifique. Además, un proceso de sincronización en segundo plano garantiza que los cambios se guardan en iCloud al cerrar la sesión.

Seguridad de iCloud y los datos

Es muy importante que los datos se guarden de forma segura cuando los alumnos creen documentos, hagan actividades de clase o realicen cursos, y también deben estar a buen recaudo en todo momento, tanto en el dispositivo como en iCloud.

Con iCloud, los documentos, contactos, notas, marcadores, eventos del calendario y recordatorios de los alumnos se guardan automáticamente. Así pueden acceder a ellos desde iOS, un Mac o el portal iCloud.com en un Mac o PC. Si el usuario inicia sesión en iCloud, las apps tienen acceso por defecto a iCloud Drive. Los usuarios pueden controlar el acceso de cada app desde Ajustes > iCloud. Los ID de Apple Gestionados tienen activados todos estos servicios por defecto.

iCloud cumple los estándares de seguridad del sector y emplea políticas estrictas de protección de datos. Para ello, iCloud los cifra antes de enviarlos a través de Internet, los almacena en un formato cifrado cuando están en el servidor y emplea tokens de seguridad para su autenticación. Esto significa que no se puede acceder a los datos de los alumnos sin autorización, ni cuando se transmiten entre dispositivos ni cuando están almacenados en la nube. iCloud usa un cifrado AES mínimo de 128 bits (el mismo nivel de seguridad que emplean la mayoría de empresas financieras) y nunca ofrece claves de cifrado a terceros. Apple conserva las claves de cifrado en sus centros de datos. Además, iCloud almacena las contraseñas y las credenciales de los alumnos de forma que Apple no pueda acceder a ellos.

Más información sobre la seguridad y privacidad de iCloud en https://support.apple.com/es-es/HT202303.

CloudKit y apps de terceros

Las apps de terceros son fundamentales en un entorno de aprendizaje moderno. Para ofrecer a los alumnos el mismo grado de seguridad al guardar y consultar sus datos en apps de terceros, hemos creado CloudKit, un entorno de software que otros desarrolladores pueden usar para almacenar y sincronizar los datos en iCloud.

En las apps compatibles con CloudKit, los estudiantes inician sesión automáticamente con su ID de Apple, así que no tienen que crear una cuenta ni proporcionar ninguna otra información. Es decir, no necesitan más nombres de usuario y contraseñas para llegar a la información que buscan. Por su parte, los desarrolladores no acceden al ID de Apple del alumno, sino a su identificador único.

Independientemente de que el desarrollador use o no CloudKit, conviene saber que las apps de terceros pueden recopilar datos del alumno. Es responsabilidad del centro cumplir con la normativa legal al usar apps de terceros. Por tanto, tu centro debe revisar las condiciones, políticas y prácticas de las apps de terceros para conocer los datos que pueden recoger de los alumnos, cómo van a usarse y si se necesita el consentimiento de los padres.

En el App Store exigimos a los desarrolladores que acepten unas directrices pensadas para salvaguardar la seguridad y la privacidad de los usuarios. Cuando detectamos que una app incumple nuestras directrices, instamos al desarrollador a que solucione el problema. Si no lo hace, lo expulsamos del App Store.

Servicios de localización y Modo Perdido

Es muy probable que a los alumnos se les pida que activen los servicios de localización según la app o el servicio que estén usando. Apple ofrece a los usuarios un control más preciso sobre cómo se gestionan sus datos de localización y cómo se comparten con apps y servicios en la nube.

Los servicios de localización permiten que las apps que los utilizan (como Mapas, Tiempo y Cámara) puedan recopilar y utilizar datos sobre la posición del usuario. En el caso de los datos de localización recogidos por Apple, no se identifican de manera personal con el alumno. Los servicios de localización están desactivados por defecto, pero se pueden activar con un simple interruptor en Ajustes. Los alumnos pueden autorizar el acceso a cada app siempre que se les pida permiso.

Cuando una app del iPad está usando los servicios de localización, aparece un icono en forma de flecha en la barra de menús. Las apps pueden solicitar datos de localización solo cuando están en uso o en todo momento, y los usuarios pueden optar por no autorizar el acceso y cambiar de opinión cuando quieran desde Ajustes. El acceso puede configurarse como Nunca, Al Usarse o Siempre, dependiendo del uso de cada app. Además, si las apps autorizadas para usar la ubicación utilizan este permiso mientras están en segundo plano, se mostrará un recordatorio para que los usuarios puedan cambiar el acceso de la app si quieren.

Los servicios de localización también sirven para ayudar a los centros a recuperar dispositivos robados o extraviados. El administrador de MDM puede activar el Modo Perdido en un dispositivo supervisado con iOS 9.3 o posterior. Al activar el Modo Perdido, se cierra la sesión abierta y no se puede desbloquear el dispositivo. La pantalla muestra un mensaje que el administrador puede cambiar, por ejemplo para incluir un número de teléfono al que llamar si encuentran el dispositivo. Con el Modo Perdido, el administrador puede solicitar que el dispositivo mande su ubicación al servidor MDM. Cuando el administrador desactiva el Modo Perdido, también se envía la ubicación del dispositivo y se informa al usuario.

Datos de diagnóstico

Si el centro o los alumnos quieren ayudarnos a mejorar nuestros productos y servicios, pueden apuntarse al programa Diagnóstico y Uso y enviarnos información no identificable sobre su dispositivo y sus aplicaciones.

Para ello es necesario enviar un consentimiento explícito. Los usuarios pueden ver los datos en su dispositivo o dejar de enviarlos en cualquier momento desde Ajustes. En el caso de los centros con iPad Compartidos, se puede desactivar el envío de Diagnóstico y Uso mediante una restricción.

iOS también incluye funciones avanzadas de diagnóstico que pueden ser útiles para depurar el dispositivo y solucionar otros problemas. Estas prestaciones no envían ningún dato a Apple sin herramientas adicionales y el consentimiento explícito.

Transferencia internacional de datos

Apple trabaja con centros educativos de todo el mundo para que los profesores lleven las mejores herramientas a las aulas.

Con Apple School Manager, los ID de Apple Gestionados, iTunes U y iCloud, los datos personales pueden almacenarse fuera del país de origen. Sea cual sea la ubicación, se aplican unas normas y requisitos igual de estrictos en cuanto al almacenamiento de datos.

Apple garantiza que los datos personales transferidos desde el Espacio Económico Europeo o Suiza a los Estados Unidos de América cumplen con los principios internacionales Safe Harbor o su sucesor (Apple Inc. cuenta con la certificación), o bien con el modelo de cláusulas contractuales o el acuerdo suizo sobre el envío transfronterizo de datos que se adjunta como anexo en el Acuerdo de Apple School Manager.

Otros recursos

La confianza de tu centro y de tus estudiantes lo es todo para nosotros. Por eso, en Apple respetamos la privacidad de los alumnos y la protegemos mediante políticas estrictas que regulan el tratamiento de todos los datos.

En estos recursos encontrarás más información y, si tienes dudas sobre la privacidad, puedes ponerte en contacto con nosotros en todo momento desde www.apple.com/es/privacy/contact.

El compromiso de Apple con tu privacidad: www.apple.com/es/privacy/

Apple en la Educación: TI e Implantación www.apple.com/es/education/it/

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

Ayuda de Apple School Manager: help.apple.com/schoolmanager/

Guía de implantación para el sector educativo: help.apple.com/deployment/education/

Guía de seguridad de iOS: http://www.apple.com/es/business/docs/iOS_Security_Guide.pdf

© 2016 Apple Inc. Todos los derechos reservados. Apple, el logotipo de Apple, Apple Pay, FaceTime, iMessage, iPad, iTunes U, Mac, Siri, Spotlight y Touch ID son marcas comerciales de Apple Inc., registradas en EE. UU. y en otros países. HomeKit es una marca comercial de Apple Inc., iCloud y iTunes Store son marcas de servicio de Apple Inc., registradas en EE. UU. y en otros países. App Store es una marca de servicio de Apple Inc. IOS es una marca comercial o una marca registrada de Cisco en EE. UU. y en otros países, y se utiliza bajo licencia. Otros nombres de productos y empresas mencionados en el presente documento pueden ser marcas comerciales de sus respectivas compañías. Las especificaciones de producto están sujetas a cambios sin previo aviso. Mayo de 2016