Apple nell'istruzione
Panoramica sulla privacy e la sicurezza dei dati per gli istituti scolastici

L'istruzione è sempre stata nel DNA di Apple. Crediamo che la tecnologia abbia il potere di trasformare l'insegnamento e l'apprendimento. I nostri prodotti sono progettati per offrire a docenti e studenti nuovi modi di insegnare e imparare fornendo loro potenti app e contenuti coinvolgenti sui dispositivi che amano usare. Sappiamo anche quanto sia importante proteggere la sicurezza e la privacy dei dati che gli studenti creano, salvano e utilizzano ogni giorno.

Sicurezza e privacy sono fondamentali nella progettazione dell'hardware, del software e dei servizi Apple, e adottiamo un approccio globale per garantire che ogni aspetto dell'esperienza d'uso sia completamente sicuro, per tutti gli utenti: anche per chi utilizza i nostri prodotti in un contesto didattico, come docenti, personale scolastico e studenti.

Inoltre, abbiamo creato funzioni e servizi pensati appositamente per il mondo dell'istruzione, tra cui Apple School Manager, gli ID Apple gestiti e gli iPad condivisi. Sono funzioni sviluppate seguendo lo stesso tipo di approccio integrato, ma con un'attenzione particolare alle esigenze di sicurezza e privacy specifiche di studenti e istituti scolastici.

Questa panoramica descrive in che modo gli ID Apple gestiti, le funzioni e i servizi dedicati all'istruzione gestiscono i dati e la privacy degli studenti; può essere usata per spiegare ai genitori che, con Apple, i dati dei loro figli sono sempre al sicuro.

L'impegno di Apple per la privacy degli studenti

Apple non registra, condivide o vende le informazioni degli studenti a scopi di marketing o per l'invio di pubblicità, né lo farà mai. Non ricostruiamo i profili degli studenti in base ai contenuti delle email o alle abitudini di navigazione sul web. Inoltre non raccogliamo, utilizziamo né divulghiamo le informazioni personali degli studenti, a meno che non siano richieste per fornire servizi didattici. Apple non vende le informazioni personali degli studenti né le divulga a scopi pubblicitari.

Per la massima trasparenza, le nostre Norme sulla privacy e il contratto Apple School Manager Agreement stabiliscono in che modo raccogliamo, usiamo, divulghiamo, trasferiamo e archiviamo le informazioni degli utenti. Abbiamo anche firmato lo Student Privacy Pledge, sottoscrivendone i principi.

Apple School Manager e gli ID Apple gestiti

Apple offre a scuole e università di ogni dimensione una gamma di servizi che semplificano la distribuzione di iPad e Mac. Si tratta di servizi progettati pensando innanzitutto alla sicurezza e alla privacy, in modo da garantire la protezione dei dati dell'istituto e degli studenti prima, durante e dopo la distribuzione.

Apple School Manager è un servizio online gratuito che offre ai responsabili tecnici tutto quel che serve per distribuire iPad e Mac nel loro istituto. Permette di acquistare contenuti, configurare la registrazione automatica nel sistema MDM per la gestione dei dispositivi mobili, creare ID Apple gestiti per studenti e personale, e preparare corsi iTunes U.

Un aspetto fondamentale di Apple School Manager è la possibilità di creare ID Apple gestiti dall'istituto. Questo nuovo tipo di ID Apple permette agli studenti di accedere ad iCloud, iTunes U e agli iPad condivisi, lasciando all'amministrazione della scuola le necessarie funzioni di controllo. Gli ID Apple gestiti sono destinati esclusivamente all'uso in ambito didattico.

Per garantire che non possano essere usati per altri scopi, abbiamo disabilitato alcune funzioni degli ID Apple gestiti. Gli studenti non possono effettuare acquisti su App Store, iBooks Store o iTunes Store. Inoltre Apple Pay, Trova i miei amici, Trova il mio iPhone, iCloud Mail, HomeKit e Portachiavi iCloud sono disattivati. Anche FaceTime e iMessage sono disabilitati di default, ma possono essere attivati da un amministratore.

Con Apple School Manager è possibile creare automaticamente gli ID Apple gestiti per gli studenti e il personale importando i dati dal Sistema Informativo di Gestione (MIS) o dai file CSV esportati dall'anagrafica dell'istituto. Ogni account viene creato con dati di sola lettura a partire dalla sorgente. Si possono aggiungere altre informazioni in Apple School Manager, come l'identificatore dell'ID Apple gestito e la password associata, ma i dati non vengono mai scritti a ritroso sul MIS.

L'account utente può contenere le seguenti informazioni, visibili nell'elenco degli account o quando l'account viene selezionato:

- ID alfanumerico associato all'account
- Nome, secondo nome e cognome
- Classe (se disponibile)
- Corsi seguiti
- Indirizzo email (se disponibile)
- Ruolo
- Ubicazione
- Fonte
- Data di creazione
- Data di modifica

Dato che gli ID Apple gestiti vengono creati e assegnati dall'istituto, l'amministrazione può agevolmente resettare le password, verificare gli account, e impostare ruoli e autorizzazioni per ciascun utente. Ogni volta che un amministratore verifica un account o viene reimpostata una password, Apple School Manager registra l'azione in modo da conservare un log dell'attività.

Gli ID Apple gestiti supportano diverse opzioni per il codice di accesso: dai codici alfanumerici più complessi a semplici sequenze di quattro cifre. Al momento della creazione o dell'importazione degli account, Apple School Manager crea password temporanee che gli utenti useranno per il primo accesso con l'ID Apple gestito: dopodiché, dovranno impostare una nuova password. In seguito, Apple School Manager non mostrerà mai la password scelta dall'utente. Lo studente può anche fare i compiti su un dispositivo non gestito dall'istituto, per esempio quando è a casa. Dovrà solo accedere usando il suo ID Apple gestito, la password e un codice di verifica a sei cifre fornito dall'amministratore mediante Apple School Manager. Il codice di verifica aggiuntivo scade dopo un anno.

Un amministratore di Apple School Manager può fornire un account ID Apple gestito che sarà accessibile a uno studente, un docente, un membro del personale o un responsabile per circa 180 giorni, dopodiché tutti i dati associati all'account saranno cancellati in modo definitivo. Qualora l'istituto richieda la cancellazione immediata di un ID Apple gestito, non sarà più possibile accedere all'account e tutte le informazioni associate all'ID verranno cancellate definitivamente entro 40 giorni.

ID Apple gestiti e iPad condivisi

Nel caso di un iPad condiviso fra più ragazzi, ogni studente può accedere con un ID Apple gestito e ritrovare subito le sue app insieme a contenuti e impostazioni. Così, anche usando un unico dispositivo, sarà comunque possibile offrire un'esperienza didattica personalizzata.

Quando uno studente accede a un iPad condiviso, l'ID Apple gestito viene autenticato automaticamente sui server Apple. Se è la prima volta che usa il dispositivo, il sistema configura una nuova home directory e un portachiavi. Il dispositivo effettua automaticamente l'accesso ad iCloud una volta creato e sbloccato l'account locale. A quel punto vengono ripristinate le impostazioni dello studente e si avvia la sincronizzazione di documenti e dati da iCloud.

Per tutto il tempo in cui la sessione dello studente rimane attiva e il dispositivo è online, i dati e i documenti creati o modificati vengono archiviati su iCloud. Inoltre, un sistema di sincronizzazione in background assicura che le modifiche vengano salvate su iCloud al momento del logout.

iCloud e sicurezza dei dati

Man mano che gli studenti creano documenti, usano i materiali didattici e partecipano alle attività di classe, è fondamentale che i loro dati vengano archiviati in modo sicuro e che siano sempre protetti, sia sui dispositivi sia su iCloud.

Con iCloud documenti, contatti, note, segnalibri, eventi di calendario e promemoria vengono salvati automaticamente, e gli utenti possono accedervi su tutti i loro dispositivi iOS e Mac o collegandosi a iCloud.com da un Mac o un PC. Se l'utente effettua il login ad iCloud, le app vengono autorizzate di default ad accedere ad iCloud Drive. È possibile controllare l'accesso delle singole app andando in Impostazioni e selezionando iCloud. Per impostazione predefinita, i servizi appena descritti sono abilitati per gli ID Apple gestiti.

iCloud include di serie procedure di sicurezza standard di settore e applica norme rigorose per la protezione dei dati. Protegge i dati degli utenti criptandoli durante la trasmissione via internet, archiviandoli in formato crittografato e utilizzando token sicuri per l'autenticazione. In questo modo i dati sono protetti dagli accessi non autorizzati sia quando vengono trasmessi sui dispositivi, sia quando sono archiviati su iCloud. Inoltre, iCloud utilizza la crittografia AES ad almeno 128 bit, lo stesso livello di sicurezza adottato dai principali istituti finanziari; le chiavi di codifica non vengono mai fornite a terzi e sono conservate nei nostri data center. E iCloud memorizza password e credenziali in modo che nemmeno Apple possa accedervi.

Per saperne di più sulla sicurezza e sulla privacy di iCloud, vai su https://support.apple.com/it-it/HT202303.

CloudKit e app di altri sviluppatori

Le app di altri sviluppatori sono un elemento essenziale di un ambiente didattico moderno. Per permettere agli studenti di memorizzare e recuperare i propri dati con la stessa semplicità anche nelle app non Apple, abbiamo creato CloudKit, un framework che gli sviluppatori possono usare per archiviare e sincronizzare i dati su iCloud.

Se un'app usa CloudKit, il login con l'ID Apple avviene in automatico: gli studenti non devono creare un altro account o fornire altri dati personali, e hanno tutte le informazioni necessarie a portata di mano, senza bisogno di ricordare un nuovo nome utente o una nuova password. Gli sviluppatori non hanno accesso all'ID Apple dello studente, ma solo a un identificatore univoco.

È importante sapere che le app di altri sviluppatori possono raccogliere dati sullo studente, a prescindere dal fatto che utilizzino CloudKit o meno. È responsabilità dell'istituto assicurare la conformità a tutte le leggi in vigore ed esaminare le condizioni, le policy e le procedure delle app di altri sviluppatori per verificare quali dati possono essere raccolti, come vengano utilizzati e se è necessario il consenso dei genitori.

Per pubblicare sull'App Store, gli sviluppatori devono adeguarsi a specifiche linee guida studiate per tutelare la privacy e la sicurezza degli utenti. Quando ci accorgiamo che un'app viola queste linee guida, lo sviluppatore deve risolvere il problema, pena la rimozione dall'App Store.

Servizi di localizzazione e modalità Smarrito

Quando usano le app e i servizi sui loro dispositivi, agli studenti verrà probabilmente richiesto di attivare i servizi di localizzazione per un'app specifica o per una determinata attività all'interno dell'app. Apple permette agli utenti di controllare con precisione il modo in cui i dati sulla loro posizione vengono gestiti e condivisi con app e servizi cloud.

I servizi di localizzazione permettono alle app basate sulla posizione, come Mappe, Meteo e Fotocamera, di raccogliere e utilizzare questo tipo di dati. Le informazioni raccolte da Apple non consentono di risalire all'identità dello studente. I servizi di localizzazione sono disattivati di default, ma è possibile abilitarli usando un unico controllo in Impostazioni; gli studenti possono anche approvare l'accesso al servizio singolarmente per ciascuna app che lo richiede.

Se un'app sull'iPad sta utilizzando i servizi di localizzazione, nella barra dei menu compare l'icona di una freccia. Le app possono richiedere l'autorizzazione a usare i dati sulla posizione solo quando sono in uso o in qualsiasi momento. Gli utenti possono scegliere di non consentire l'accesso, e anche modificare la propria scelta in Impostazioni. È possibile impostare l'accesso su Mai, "Mentre usi l'app" o Sempre, a seconda dell'app. Inoltre, se le app autorizzate accedono ai dati sulla posizione mentre sono in background, un messaggio permetterà all'utente di modificare la sua scelta.

Gli istituti scolastici possono usare i servizi di localizzazione anche per recuperare un dispositivo perso o rubato. Su un dispositivo supervisionato con iOS 9.3 o successivo, l'amministratore MDM può attivare in remoto la modalità Smarrito, che forza il logout dell'utente attuale e impedisce di sbloccare il dispositivo. Lo schermo mostra un messaggio che può essere personalizzato dall'amministratore, per esempio con un numero di telefono da chiamare in caso di ritrovamento. In modalità Smarrito, l'amministratore può richiedere al dispositivo di segnalare la propria posizione al server MDM. Se un amministratore disattiva la modalità Smarrito per un dispositivo, anche in quel caso verranno inviati i dati sulla posizione e l'utente sarà informato.

Dati di diagnosi

Insegnanti e studenti possono contribuire a migliorare i prodotti e i servizi Apple scegliendo di partecipare al nostro programma "Diagnosi e uso" per fornirci informazioni non identificabili sul dispositivo e le applicazioni.

È richiesto un consenso esplicito per farlo. Gli utenti possono in qualsiasi momento visualizzare i dati sul loro dispositivo o interrompere l'invio dei dati in Impostazioni; per le distribuzioni con iPad condivisi, l'istituto può disattivare l'invio dei dati di diagnosi e uso mediante una restrizione.

iOS offre anche funzioni diagnostiche evolute utili per la correzione dei bug e la risoluzione dei problemi sui dispositivi. Queste funzioni non inviano dati a Apple senza l'utilizzo di altri strumenti e senza l'esplicito consenso dell'utente.

Trasferimento internazionale di dati

Apple collabora con istituti scolastici in tutto il mondo per offrire a insegnanti e studenti i migliori strumenti per l'apprendimento.

Con Apple School Manager, gli ID Apple gestiti, iTunes U e iCloud, i dati personali potrebbero essere archiviati al di fuori del Paese di origine. Indipendentemente dall'ubicazione, verranno sempre applicati gli stessi rigorosi standard e requisiti in materia di archiviazione.

Apple garantisce che i dati personali trasferiti dallo Spazio economico europeo o la Svizzera agli Stati Uniti d'America sono disciplinati da un Programma Safe Harbor in vigore o da un eventuale programma successivo per il quale Apple Inc. è certificata, oppure dai documenti "Model Contractual Clauses" e "Swiss Transborder Data Flow Agreement" allegati all'Apple School Manager Agreement.

Risorse aggiuntive

Per Apple, la fiducia degli istituti scolastici e degli studenti è tutto. Per questo rispettiamo la privacy degli utenti e la proteggiamo con norme rigorose che disciplinano il trattamento di tutti i dati.

Per maggiori informazioni, consulta le risorse aggiuntive qui sotto. Se hai domande sulla privacy puoi contattarci direttamente da http://www.apple.com/it/privacy/contact.

L'impegno di Apple per la tua privacy: http://www.apple.com/it/privacy/

Apple Education: IT e distribuzione http://www.apple.com/it/education/it/

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

Aiuto di Apple School Manager: https://help.apple.com/schoolmanager/

Guida alla distribuzione nell'istruzione: https://help.apple.com/deployment/education/

Sicurezza di iOS: http://www.apple.com/it/business/docs/iOS_Security_Guide.pdf