Apple in het onderwijs
Overzicht voor scholen over de privacy van gegevens

Bij Apple staat het onderwijs sinds jaar en dag hoog in het vaandel. Wij zijn ervan overtuigd dat technologie elk klaslokaal kan transformeren en elke leerling verder kan helpen. Onze producten zijn zo gemaakt dat ze leerkrachten en leerlingen meer mogelijkheden geven, want ze bieden hun toegang tot veelzijdige apps en aansprekende content. We weten ook hoe belangrijk privacy is en dat alle gegevens die leerlingen aanmaken, bewaren en raadplegen, goed moeten worden afgeschermd.

Beveiliging en privacy zijn fundamentele elementen in het ontwerp van alle hardware, software en voorzieningen van Apple. We pakken dit op een geïntegreerde manier aan, om de beveiliging en privacy zo goed mogelijk te waarborgen. Die aanpak is berekend op alle soorten gebruikers, ook binnen een onderwijssetting, zoals leerkrachten, andere medewerkers op een school en leerlingen.

Daarnaast hebben we speciale functies en voorzieningen voor het onderwijs ontwikkeld, namelijk Apple School Manager, beheerde Apple ID's en Gedeelde iPad. Bij het ontwerp hebben we dezelfde geïntegreerde aanpak gebruikt, met extra aandacht voor de specifieke beveiligings- en privacyeisen in het onderwijs.

In dit overzicht wordt uitgelegd hoe beheerde Apple ID's en de bijbehorende onderwijsfuncties en -voorzieningen omgaan met de gegevens van leerlingen en hun privacy. Je kunt uit dit overzicht putten als je ouders wilt informeren over hoe Apple de gegevens van hun kind afschermt.

Wat Apple doet om de privacy van leerlingen te beschermen

Apple zal nooit gegevens van leerlingen bijhouden, delen of verkopen voor reclame- of marketingdoeleinden. We stellen geen profielen op van leerlingen op basis van hun e-mails of surfgedrag. Voor zover we persoonlijke gegevens van leerlingen verzamelen, gebruiken of vrijgeven, doen we dat alleen binnen het kader van onze diensten en voorzieningen. Apple zal nooit persoonlijke gegevens van leerlingen verkopen of vrijgeven voor gerichte reclamedoeleinden.

In het Apple privacybeleid plus de Apple School Manager-overeenkomst is vastgelegd hoe we gegevens van gebruikers verzamelen, gebruiken, vrijgeven, overdragen en bewaren. Verder hebben we de Student Privacy Pledge ondertekend.

Apple School Manager en beheerde Apple ID's

Apple reikt scholen en instellingen in alle soorten en maten voorzieningen aan om de implementatie van iPad en Mac te vergemakkelijken. Al bij de ontwikkeling van deze voorzieningen is rekening gehouden met beveiliging en privacy. Hierdoor zijn de gegevens van je instelling en van de leerlingen voor, tijdens en na de implementatie goed afgeschermd.

Apple School Manager is een gratis webvoorziening waarmee IT-beheerders alles kunnen regelen voor de implementatie van iPad en Mac op school. Ze kunnen er content kopen, de automatische aanmelding in de MDM-oplossing configureren, accounts aanmaken voor de leerlingen en andere gebruikers, en iTunes U-cursussen klaarzetten.

Een belangrijke functie van Apple School Manager is het aanmaken van beheerde Apple ID's. Beheerde Apple ID's zijn een nieuw soort ID. Hiermee geef je leerlingen toegang tot iCloud, iTunes U en Gedeelde iPad, terwijl je als school toch de touwtjes in handen houdt. Beheerde Apple ID's zijn specifiek voor het onderwijs bedoeld.

Om ervoor te zorgen dat leerlingen de devices die hun school ter beschikking stelt alleen gebruiken voor hun schoolwerk, hebben we bepaalde functies van beheerde Apple ID-accounts uitgeschakeld. Zo kunnen leerlingen geen aankopen doen in de App Store, iBooks Store of iTunes Store. Verder zijn Apple Pay, Zoek mijn vrienden, Zoek mijn iPhone, iCloud-mail, HomeKit en iCloud-sleutelhanger uitgeschakeld. FaceTime en iMessage staan ook standaard uit, maar kunnen door een beheerder worden ingeschakeld.

In Apple School Manager kun je beheerde Apple ID's automatisch laten genereren voor alle leerlingen en leerkrachten. Je importeert dan alleen de benodigde gegevens vanuit het managementinformatiesysteem (MIS) of vanuit csv-bestanden die uit adressenlijsten zijn geëxporteerd. Elke gebruikersaccount wordt aangemaakt met niet-bewerkbare gegevens uit het bronbestand. Aanvullende informatie, zoals de identificatiecode van de beheerde Apple ID en het bijbehorende wachtwoord, wordt in Apple School Manager toegevoegd aan de accountgegevens. Er worden in geen geval gegevens naar het MIS geschreven.

Aan elke gebruikersaccount kan de onderstaande informatie gekoppeld zijn, die te zien is in de accountlijst of bij het selecteren van een specifieke account:

- Een unieke alfanumerieke code
- Voornaam, tweede naam en achternaam
- Klas of groep (indien ingevoerd)
- Aangemelde klassen
- E-mailadres (indien ingevoerd)
- Rol
- Locatie
- Bron
- Datum aangemaakt
- Datum gewijzigd

De school maakt deze beheerde Apple ID's zelf aan en wijst ze ook zelf toe. Daarom is het heel eenvoudig om wachtwoorden te resetten, accounts te inspecteren en rollen te definiëren. Zodra een beheerder een account inspecteert of een wachtwoord wordt gereset, wordt dit automatisch vastgelegd in een logboek. Zo kun je altijd nagaan wat er precies is gebeurd.

Beheerde Apple ID's ondersteunen allerlei soorten toegangscodes, van eenvoudige codes van vier cijfers tot complexe alfanumerieke combinaties. Apple School Manager stelt een tijdelijk wachtwoord in voor nieuw aangemaakte of geïmporteerde accounts. Daarmee kunnen gebruikers voor de eerste keer inloggen, waarna ze meteen een ander wachtwoord moeten instellen. Zodra een leerling dit heeft gedaan, laat Apple School Manager nooit het nieuwe wachtwoord zien. Leerlingen kunnen ook bij hun bestanden van school op een device dat niet door de instelling wordt beheerd, bijvoorbeeld op een device thuis. Ze loggen dan in met hun beheerde Apple ID, wachtwoord en een verificatiecode van zes cijfers die de beheerder via Apple School Manager heeft toegewezen. Deze verificatiecode verloopt automatisch na één jaar.

Een Apple School Manager-beheerder kan een beheerde Apple ID-account vrijgeven. Die account is dan ongeveer 180 dagen toegankelijk voor de leerling, de leerkracht, een andere medewerker van de school of een manager. Daarna worden alle gegevens van die account definitief verwijderd. Als een beheerde Apple ID direct wordt verwijderd, is de account niet meer toegankelijk en worden alle bijbehorende gegevens binnen 40 dagen definitief verwijderd.

Beheerde Apple ID's en Gedeelde iPad

Als leerlingen een iPad met elkaar moeten delen, loggen ze in met een beheerde Apple ID. Zo kunnen ze altijd werken met hun eigen apps, content en instellingen. Op deze manier kunnen meerdere leerlingen dezelfde iPad gebruiken, want ze werken allemaal in hun eigen gedeelte.

Zodra een leerling inlogt bij Gedeelde iPad, wordt de beheerde Apple ID automatisch geverifieerd met de identiteitsservers van Apple. Als de leerling dat device voor het eerst gebruikt, worden automatisch een nieuwe thuismap en sleutelhanger voor die gebruiker aangemaakt. Zodra de lokale account van de leerling is aangemaakt en ontgrendeld, wordt het device automatisch aangemeld bij iCloud. Vervolgens worden de instellingen van de leerling bewaard en worden documenten en gegevens gesynchroniseerd vanuit iCloud.

Zolang een sessie actief is en het device online blijft, worden alle documenten en gegevens bewaard in iCloud zodra ze worden aangemaakt of gewijzigd. Op de achtergrond loopt nog een synchronisatieproces dat ervoor zorgt dat alle wijzigingen in iCloud worden bewaard wanneer de leerling uitlogt.

iCloud en gegevensbeveiliging

Terwijl de leerlingen nieuwe documenten aanmaken, interactief met hun lessen werken en meedoen aan klassikale activiteiten, is het belangrijk dat ze alles veilig en goed afgeschermd kunnen bewaren, zowel op het device zelf als in iCloud.

Dankzij iCloud worden al hun documenten, contactgegevens, notities, bladwijzers, agenda's en herinneringen automatisch bewaard. Bovendien hebben ze er altijd toegang toe op hun iOS-device en Mac, plus via iCloud.com op een Mac of pc. Zodra een gebruiker zich aanmeldt bij iCloud, krijgen apps standaard toegang tot iCloud Drive. De gebruiker kan deze toegang per app instellen onder 'Instellingen' > 'iCloud'. Voor beheerde Apple ID's zijn de bovenstaande voorzieningen standaard ingeschakeld.

iCloud is ontwikkeld volgens gangbare beveiligingsnormen en werkt met strenge gegevensbeveiligingsprotocollen. iCloud beveiligt gebruikersgegevens door deze te coderen voordat ze via het internet worden verzonden, door ze gecodeerd te bewaren op de server en door veilige tokens te gebruiken voor identiteitscontrole. Dit betekent dat de gegevens van leerlingen beschermd zijn tegen onbevoegde toegang wanneer ze naar een device worden verzonden en wanneer ze in iCloud worden bewaard. iCloud maakt gebruik van minimaal 128-bits AES-versleuteling, dezelfde beveiliging die in gebruik is bij grote financiële instellingen. Coderingssleutels worden in de datacenters van Apple bewaard en worden nooit doorgegeven aan derden. iCloud bewaart verder de wachtwoorden en verificatiegegevens van leerlingen op zo'n manier dat Apple ze niet kan lezen en er geen toegang toe heeft.

Ga voor meer informatie over beveiliging en privacy met betrekking tot iCloud naar https://support.apple.com/nl-nl/HT202303.

CloudKit en apps van andere ontwikkelaars

Apps van andere ontwikkelaars zijn onontbeerlijk in een moderne leeromgeving. We willen dat leerlingen ook in die apps naadloos hun gegevens kunnen bewaren en ophalen. Daarom hebben we CloudKit gemaakt, een framework dat andere ontwikkelaars kunnen gebruiken om gegevens te bewaren en te synchroniseren naar iCloud.

In een app die CloudKit gebruikt, worden leerlingen automatisch aangemeld met hun Apple ID. Ze hoeven dus geen nieuwe account aan te maken of andere persoonlijke informatie in te voeren. Zo hebben ze altijd toegang tot de meest actuele informatie in de app zonder dat ze een andere gebruikersnaam of een ander wachtwoord hoeven te onthouden. Ontwikkelaars hebben geen toegang tot de Apple ID van leerlingen, alleen tot een unieke identificatiecode.

Ongeacht het feit of een ontwikkelaar CloudKit wel of niet gebruikt, het is altijd mogelijk dat apps van andere ontwikkelaars gegevens over leerlingen verzamelen. Het is de taak van de school om erop toe te

zien dat alle relevante wet- en regelgeving wordt nageleefd bij het gebruik van apps van andere ontwikkelaars. De school moet zich goed verdiepen in de voorwaarden, beleidsteksten en werking van dit soort apps, en dan met name nagaan of er gegevens van leerlingen worden verzameld, wat daarmee wordt gedaan en of de toestemming van ouders vereist is.

Ontwikkelaars die hun app via onze App Store willen distribueren, moeten akkoord gaan met specifieke richtlijnen die zijn opgesteld om de privacy en veiligheid van de gebruiker te garanderen. Als we ontdekken dat een app deze richtlijnen schendt, moet de ontwikkelaar het probleem oplossen. Als dat niet gebeurt, wordt de app uit de App Store verwijderd.

Locatievoorzieningen en Verloren-modus

Bij het gebruik van de apps en voorzieningen op hun device krijgen leerlingen vroeg of laat de vraag voorgeschoteld of ze locatievoorzieningen willen inschakelen. Apple geeft gebruikers de optie om heel gericht in te stellen wat er met hun locatiegegevens gebeurt en in hoeverre die worden gedeeld met apps en cloudvoorzieningen.

Met de functie 'Locatievoorzieningen' kunnen locatiegerichte apps (zoals Kaarten, Weer en Camera) locatiegegevens verzamelen en gebruiken. Uit de locatiegegevens die Apple verzamelt, is niet te herleiden van welke specifieke leerling ze afkomstig zijn. Locatievoorzieningen is standaard uitgeschakeld, maar kan in 'Instellingen' met één tikje worden aangezet. Leerlingen kunnen voor alle desbetreffende apps per app de gewenste toegang instellen.

Als een app op iPad gebruikmaakt van Locatievoorzieningen, zie je in de menubalk het symbool van een pijl staan. Zo'n app kan dan ofwel vragen om permanente toegang tot je locatie ofwel alleen bij gebruik. Gebruikers kunnen die toegang ook weigeren en hun keuze in 'Instellingen' aanpassen. Ze kunnen dan kiezen om het nooit toe te staan, alleen bij gebruik of altijd, afhankelijk van de app. Bovendien krijg je een melding als een app je locatiegegevens op de achtergrond gebruikt, ook als je daar toestemming voor hebt gegeven. Je kunt je keuze dan alsnog aanpassen.

De functie 'Locatievoorzieningen' speelt ook een rol bij het terugvinden van een device dat kwijt is of is gestolen. Op een device onder supervisie met iOS 9.3 of hoger kan een MDM-beheerder op afstand de Verloren-modus inschakelen. De gebruiker wordt dan uitgelogd en het device kan niet meer worden ontgrendeld. Op het scherm wordt een melding weergegeven die door de beheerder kan worden aangepast. Denk bijvoorbeeld aan het verzoek om een bepaald telefoonnummer te bellen wanneer iemand het device vindt. De beheerder kan een device in de Verloren-modus een verzoek sturen om de huidige locatie door te geven aan de MDM-server. Wanneer een beheerder de Verloren-modus uitschakelt, wordt de locatie van het device ook verzonden en wordt dat gemeld aan de gebruiker.

Diagnostische gegevens

Als jij en je leerlingen ons willen helpen de producten en diensten van Apple te verbeteren, kun je je aanmelden bij ons diagnose- en gebruiksprogramma. Er wordt dan niet-identificeerbare informatie over jullie devices en apps naar Apple gestuurd.

Hiervoor moet je expliciet toestemming geven. Gebruikers kunnen deze gegevens inzien op hun device of het verzenden daarvan altijd stopzetten in 'Instellingen'. Als je school gebruikmaakt van gedeelde iPads, kan het versturen van diagnose- en gebruiksgegevens via een beperking worden uitgeschakeld.

iOS bevat ook geavanceerde diagnostische voorzieningen die nuttig kunnen zijn bij het opsporen van fouten of het oplossen van problemen met devices. Deze geavanceerde diagnostische voorzieningen versturen geen gegevens naar Apple zonder aanvullende hulpprogramma's en uitdrukkelijke goedkeuring.

Internationale gegevensoverdracht

Apple werkt met scholen over de hele wereld om leerkrachten en klaslokalen te voorzien van de beste onderwijstools.

Wanneer gebruik wordt gemaakt van Apple School Manager, beheerde Apple ID's, iTunes U en iCloud, kan het voorkomen dat persoonlijke gegevens ergens buiten het land van oorsprong worden opgeslagen. Dat maakt op zich niet uit, want overal gelden dezelfde strenge normen en eisen voor gegevensopslag.

Apple waarborgt dat persoonlijke gegevens die vanuit de EER of Zwitserland naar de VS worden verzonden, onderworpen zijn aan een geldig Safe Harbor-akkoord (of de opvolger daarvan) dat Apple Inc. heeft ondertekend, of aan modelcontracten/een Zwitserse overeenkomst voor grensoverschrijdende gegevensstromen die als bijlage zijn toegevoegd aan de Apple School Manager-overeenkomst.

Aanvullende informatie

Voor Apple is het van cruciaal belang dat je school en je leerlingen op ons kunnen vertrouwen. Daarom respecteren we de privacy van leerlingen en beschermen we die met een strikt beleid waarin is vastgelegd hoe er met al hun gegevens wordt omgegaan.

Lees de informatiebronnen hieronder als je nog meer wilt weten. Heb je specifieke vragen over privacy? Dan kun je ons altijd rechtstreeks benaderen via www.apple.com/nl/privacy/contact.

Apple's toewijding aan jouw privacy: www.apple.com/nl/privacy/

Apple en het onderwijs – IT en implementatie: www.apple.com/nl/education/it/

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

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

Implementatiehandleiding voor het onderwijs: help.apple.com/deployment/education/

Handleiding 'iOS-beveiliging': www.apple.com/nl/business/docs/iOS_Security_Guide.pdf