



Apple w edukacji

Omówienie ochrony danych i prywatności przeznaczone dla szkół

Zastosowania edukacyjne zawsze były i są niezwykle ważne dla Apple. Jesteśmy przekonani, że technologia może zmieniać szkołę na lepsze i stwarzać uczniom warunki do większego zaangażowania w naukę. Nasze produkty wzbogacają proces nauczania i zdobywania wiedzy, dając uczniom i nauczycielom dostęp do fantastycznych aplikacji i ciekawych treści na urządzeniach, których wszyscy chętnie używają. Jednocześnie zdajemy sobie sprawę, jak ważna jest ochrona prywatności uczniów oraz danych, które uczniowie tworzą, przechowują i wykorzystują.

Bezpieczeństwo i prywatność to fundamenty, na których Apple projektuje swoje urządzenia, oprogramowanie i usługi. Kierujemy się kompleksową strategią, zgodnie z którą ochrona danych i prywatności musi być uwzględniona we wszystkich aspektach funkcjonowania produktów. Strategię tę stosujemy w odniesieniu do wszystkich użytkowników, także tych z sektora edukacji, w tym uczniów, nauczycieli i innych pracowników szkoły.

Opracowaliśmy szereg funkcji i usług przeznaczonych wyłącznie do zastosowań edukacyjnych, takich jak Apple School Manager, nadzorowane identyfikatory Apple ID i Wspólny iPad. Również one działają zgodnie z naszą kompleksową strategią bezpieczeństwa oraz ze szczególnym uwzględnieniem potrzeb uczniów i instytucji edukacyjnych w dziedzinie ochrony danych i prywatności.

W niniejszym omówieniu przedstawiono zasady postępowania z danymi i ochrony prywatności uczniów stosowane w oprogramowaniu obsługującym nadzorowane identyfikatory Apple ID oraz w powiązanych funkcjach i usługach Apple dla sektora edukacji. Omówienie to można też wykorzystać jako źródło informacji dla rodziców — by mogli się dowiedzieć, jak Apple chroni dane uczniów.

Zobowiązanie Apple do ochrony prywatności uczniów

Apple nigdy nie śledzi, nie udostępnia i nie sprzedaje informacji o uczniach w celach reklamowych lub marketingowych. Nie tworzymy profili uczniów na podstawie treści ich korespondencji e-mailowej ani tego, co i jak przeglądają w Internecie. Ponadto nie zbieramy, nie wykorzystujemy ani nie ujawniamy danych osobowych uczniów w celach niezwiązanych ze świadczeniem usług edukacyjnych. Apple nie będzie sprzedawać danych osobowych uczniów ani ujawniać informacji o uczniach w celu kierowania do nich sprofilowanych przekazów reklamowych.

Na potwierdzenie swoich zobowiązań firma Apple sformułowała [Zasady ochrony prywatności](#) oraz [Umowę o korzystanie z portalu Apple School Manager](#). W dokumentach tych szczegółowo opisano stosowane przez Apple procedury zbierania, wykorzystywania, ujawniania, przekazywania i przechowywania danych użytkowników. Apple jest również sygnatariuszem [Zobowiązań do ochrony prywatności uczniów](#).

Apple School Manager i nadzorowane identyfikatory Apple ID

Apple oferuje szkołom i innym instytucjom — zarówno dużym, jak i mniejszym — usługi ułatwiające wdrażanie iPadów i komputerów Mac. Usługi te świadczone są z zachowaniem zasad bezpieczeństwa i ochrony prywatności, by dane Państwa instytucji i uczniów były bezpieczne przed wdrożeniem, w trakcie wdrożenia i po wdrożeniu.

Apple School Manager to bezpłatny portal WWW, który udostępnia wszystko, czego szkolnym informatykom potrzeba do wdrożenia iPadów i Maców. Apple School Manager umożliwia kupowanie treści, konfigurowanie automatycznej rejestracji urządzeń w systemie zarządzania urządzeniami mobilnymi

(MDM — mobile device management), zakładanie kont dla uczniów i pracowników oraz konfigurowanie kursów iTunes U.

Jedną z kluczowych funkcji portalu Apple School Manager jest obsługa nadzorowanych identyfikatorów Apple ID, nad którymi pieczę sprawuje samodzielnie instytucja edukacyjna. Nadzorowane identyfikatory Apple ID to nowy rodzaj identyfikatorów Apple ID, które pozwalają uczniom uzyskiwać dostęp do iCloud czy iTunes U, a także wspólnie korzystać z iPada. Natomiast szkoła zachowuje nadzór nad uczniami i ich działaniami. Nadzorowane identyfikatory Apple ID są przeznaczone tylko do zastosowań edukacyjnych.

Aby nadzorowane identyfikatory Apple ID na urządzeniach udostępnionych uczniom były faktycznie używane tylko do celów edukacyjnych, celowo pozbawiliśmy ich niektórych funkcji. Uczniowie nie mogą za ich pomocą dokonywać zakupów w App Store, iBooks Store ani w iTunes Store. Ponadto wyłączone są funkcje Apple Pay, Znajdź moich znajomych, Znajdź mój iPhone, iCloud Mail, HomeKit i Pęk kluczy iCloud. Domyślnie wyłączone są także usługi FaceTime i iMessage, ale administrator może je włączyć.

Apple School Manager pozwala automatycznie tworzyć nadzorowane identyfikatory Apple ID dla wszystkich uczniów i pracowników poprzez zaimportowanie wyłącznie niezbędnych danych z systemu informacji o uczniach (Student Information System — SIS) lub plików CSV wyeksportowanych z usługi katalogowej szkoły. Każde konto użytkownika zakładane jest na podstawie informacji źródłowych, których nie można zmienić. W portalu Apple School Manager dane konta uzupełniane są o dodatkowe informacje, takie jak nadzorowany identyfikator Apple ID i skojarzone z nim hasło. Dane te nie są nigdy zapisywane w szkolnym systemie SIS.

Z każdym kontem mogą być powiązane następujące informacje widoczne na liście kont lub po wybraniu konta:

- Alfnumeryczny unikalny identyfikator przypisany do konta
- Imię, drugie imię i nazwisko
- Klasa (rok nauki), jeśli ta informacja została podana
- Zajęcia, na które uczeń jest zapisany
- Adres e-mail, jeśli został podany
- Rola
- Miejsce
- Źródło
- Data utworzenia
- Data modyfikacji

Ponieważ nadzorowane identyfikatory Apple ID są tworzone i przydzielane przez Państwa instytucję, można łatwo resetować hasła, kontrolować konta i przydzielać role wszystkim osobom w szkole lub innej organizacji. Każda kontrola konta lub operacja zresetowania hasła wykonana przez administratora jest rejestrowana przez portal Apple School Manager, zatem zachowywany jest zapis wszystkich działań.

Dla nadzorowanych identyfikatorów Apple ID można konfigurować różne warianty haseł — od prostych kodów czterocyfrowych po złożone hasła alfanumeryczne. Dla nowo zaimportowanych i założonych kont Apple School Manager tworzy hasła tymczasowe. Służą one tylko do pierwszego logowania przy użyciu nadzorowanego identyfikatora Apple ID — po pierwszym zalogowaniu użytkownik musi zmienić hasło. Apple School Manager nigdy nie wyświetla hasła, na które uczeń zmienił swoje początkowe hasło tymczasowe. Uczeń może zalogować się z urządzenia nienadzorowanego przez instytucję, na przykład z prywatnego urządzenia w domu, aby uzyskać dostęp do swoich szkolnych prac. W tym celu wprowadza hasło swojego nadzorowanego identyfikatora Apple ID i sześciocyfrowy kod weryfikacyjny podany przez administratora za pośrednictwem portalu Apple School Manager. Ten dodatkowy kod weryfikacyjny jest ważny przez jeden rok.

Administrator portalu Apple School Manager może wycofać identyfikator Apple ID spod nadzoru — spowoduje to, że konto będzie dostępne dla ucznia, nauczyciela, pracownika lub menedżera jeszcze przez około 180 dni, a następnie wszystkie dane z nim związane zostaną trwale usunięte. Jeśli instytucja nakaze natychmiastowe usunięcie nadzorowanego identyfikatora Apple ID, konto od razu stanie się niedostępne, a wszelkie informacje skojarzone z danym identyfikatorem zostaną trwale usunięte przed upływem 40 dni.

Nadzorowane identyfikatory Apple ID i Wspólny iPad

Jeśli uczniowie korzystają ze wspólnych iPadów, mogą logować się do nich za pomocą nadzorowanych identyfikatorów Apple ID, by szybko uzyskiwać dostęp do swoich aplikacji, treści i ustawień. Dzięki temu, choć z tego samego iPada korzystają różni uczniowie, każdy z nich może na nim uczyć się tak, jak gdyby było to jego własne urządzenie.

Gdy uczeń loguje się na wspólnym iPadzie, nadzorowany identyfikator Apple ID jest automatycznie uwierzytelniany na serwerach tożsamości Apple. Jeśli uczeń nie używał jeszcze danego urządzenia, tworzony jest dla niego nowy katalog domowy i pęk kluczy. Po utworzeniu i odblokowaniu lokalnego konta dla ucznia urządzenie automatycznie loguje się w iCloud. Następnie odtwarzane są ustawienia ucznia, a jego dokumenty i dane są pobierane z chmury iCloud.

W trakcie sesji ucznia, jeśli tylko urządzenie ma połączenie z siecią, tworzone lub modyfikowane dokumenty i dane są na bieżąco zapisywane w iCloud. Ponadto działający w tle mechanizm synchronizacji gwarantuje zapisanie zmian w iCloud po wylogowaniu ucznia.

iCloud i bezpieczeństwo danych

Uczniowie tworzący dokumenty oraz interaktywnie uczestniczący w lekcjach i ćwiczeniach muszą mieć możliwość bezpiecznego przechowywania danych — zarówno w urządzeniach, jak i w chmurze iCloud.

Dokumenty, kontakty, notatki, zakładki, wydarzenia w kalendarzach i przypomnienia mogą być automatycznie zapisywane w iCloud i dostępne na urządzeniach iOS, komputerach Mac oraz w witrynie [iCloud.com](https://www.icloud.com) na komputerach Mac lub PC. Gdy użytkownik jest zalogowany do iCloud, aplikacje mają domyślnie dostęp do iCloud Drive. Użytkownik może sterować dostępem poszczególnych aplikacji w Ustawieniach, w sekcji iCloud. Dla powyższych usług domyślnie są włączone nadzorowane identyfikatory Apple ID.

W chmurze iCloud stosowane są procedury bezpieczeństwa zgodne ze standardami branżowymi oraz ściśle zasady ochrony danych. iCloud szyfruje dane użytkowników, gdy są one przesyłane w Internecie, przechowuje je na serwerze w zaszyfrowanym formacie i korzysta z zabezpieczonych znaczników przy uwierzytelnianiu. Oznacza to, że dane uczniów są chronione przed dostępem osób nieupoważnionych zarówno w trakcie przesyłania, jak i na serwerach chmury iCloud. iCloud stosuje szyfrowanie AES z kluczem co najmniej 128-bitowym — czyli ten sam poziom ochrony co poważne instytucje finansowe — a klucze szyfrowania nigdy nie są udostępniane podmiotom zewnętrznym. Apple przechowuje klucze szyfrowania we własnych centrach danych. iCloud przechowuje ponadto hasła i dane uwierzytelniające użytkowników w taki sposób, że nawet firma Apple nie może ich odczytać ani uzyskać do nich dostępu.

Więcej informacji na temat bezpieczeństwa i ochrony prywatności w iCloud można znaleźć w artykule <https://support.apple.com/pl-pl/HT202303>.

CloudKit i aplikacje innych firm

Aplikacje producentów i autorów niezależnych od Apple są niezwykle ważnym składnikiem nowoczesnego środowiska dydaktycznego. Aby zapewnić uczniom możliwość wygodnego zapisywania danych w chmurze i odczytywania danych z chmury, opracowaliśmy CloudKit — architekturę, za pośrednictwem której twórcy aplikacji mogą programować procesy zapisywania i synchronizacji danych w chmurze iCloud.

W aplikacjach korzystających z CloudKit uczniowie są automatycznie logowani przy użyciu swoich Apple ID, a zatem nie muszą zakładać nowych kont ani podawać innych danych osobowych. Zawsze mają w aplikacji dostęp do swoich aktualnych informacji — bez konieczności zapamiętywania nowych nazw użytkowników i haseł. Aplikacja nie ma dostępu do Apple ID ucznia, a jedynie do unikalnego identyfikatora.

Należy pamiętać, że niezależnie od tego, czy twórca aplikacji korzystał z CloudKit, czy nie, aplikacja może zbierać dane dotyczące ucznia. Na szkole spoczywa obowiązek przestrzegania wszelkich obowiązujących przepisów w związku z wykorzystaniem aplikacji innych firm. Odpowiednie osoby w szkole powinny zapoznać się z warunkami używania aplikacji innych firm, obowiązującymi w nich zasadami i stosowanymi praktykami, aby dowiedzieć się, jakie dane o uczniach zbierają aplikacje, jak je wykorzystują i czy wymagane jest w związku z tym uzyskanie zgody rodziców lub opiekunów.

Od twórców aplikacji udostępnianych w App Store Apple wymaga zobowiązania do przestrzegania określonych wytycznych, które służą ochronie prywatności i zapewnieniu bezpieczeństwa użytkowników. Gdy uzyskamy informację o tym, że jakaś aplikacja jest niezgodna z tymi wytycznymi, jej twórca musi wyeliminować niezgodność, jeśli aplikacja ma być nadal dostępna w App Store.

Usługi lokalizacji i tryb Utracony

Korzystając z oprogramowania i usług na urządzeniach, uczniowie prawdopodobnie będą spotykać się z prośbami o włączenie usług lokalizacji — zgłaszanymi przez niektóre aplikacje lub funkcje aplikacji. Apple zapewnia użytkownikom możliwość szczegółowego sterowania wykorzystaniem danych o położeniu urządzenia i udostępnianiem ich aplikacjom oraz usługom chmurowym.

Usługi lokalizacji umożliwiają aplikacjom, w których istotne jest miejsce użycia urządzenia — takim jak Mapy, Pogoda i Aparat — zbieranie i wykorzystanie danych o położeniu. Postać, w jakiej Apple zbiera dane o położeniu, wyklucza możliwość identyfikacji tożsamości konkretnego ucznia. Usługi lokalizacji są domyślnie wyłączone, ale można je włączyć, przestawiając jeden przełącznik w Ustawieniach. Każdej aplikacji, która o to poprosi, uczeń może zezwolić bądź nie zezwolić na korzystanie z Usług lokalizacji.

Gdy aplikacja na iPadzie korzysta z Usług lokalizacji, na pasku menu widoczna jest ikona w postaci strzałki. Aplikacje mogą prosić o dostęp do danych o lokalizacji tylko w czasie, gdy są aktywnie używane, albo przez cały czas. Użytkownik może nie zezwolić na taki dostęp, a swoją decyzję może zmienić w Ustawieniach. Do wyboru dostępne są ustawienia Nigdy, Gdy używam albo Zawsze — zależnie od tego, o jaki zakres dostępu do danych o lokalizacji prosi aplikacja. Ponadto, jeśli aplikacje, którym zezwolono na dostęp do danych o lokalizacji, korzystają z tego dostępu podczas pracy w tle, wyświetlane jest przypomnienie o udzielonym zezwoleniu, a użytkownik może w dowolnej chwili zmienić swoją decyzję.

Usługi lokalizacji pomagają także w odzyskaniu zgubionych lub skradzionych urządzeń. W nadzorowanym urządzeniu z systemem iOS 9.3 lub nowszym administrator MDM może zdalnie włączyć tryb Utracony. Z chwilą włączenia tego trybu bieżący użytkownik zostaje wylogowany i od tej pory urządzenia nie można odblokować. Na ekranie wyświetlany jest komunikat zdefiniowany przez administratora, np. prośba do znalazcy urządzenia o kontakt telefoniczny pod wskazanym numerem. Administrator może zażądać, aby urządzenie przełączone w tryb Utracony wysłało dane o swojej lokalizacji do serwera MDM. Dane o lokalizacji są także wysyłane, gdy administrator wyłącza tryb Utracony; użytkownik jest wówczas o tym informowany.

Dane diagnostyczne

Instytucje i uczniowie, którzy chcieliby pomóc w doskonaleniu produktów i usług Apple, mogą zapisać się do naszego programu „Diagnostyka i użycie”, co spowoduje, że do Apple przesyłane będą informacje o ich urządzeniach i aplikacjach; informacje te nie będą jednak umożliwiały identyfikacji konkretnych osób.

Udział w tym programie wymaga wyraźnej zgody użytkownika. Użytkownik może przeglądać dane na swoim urządzeniu lub w dowolnej chwili przerwać wysyłanie danych za pośrednictwem Ustawień, a w przypadku wdrożeń wspólnych iPadów szkoła może wyłączyć przekazywanie danych diagnostycznych i dotyczących użycia, wprowadzając odpowiednie ograniczenie.

System iOS także jest wyposażony w zaawansowane funkcje diagnostyczne, które mogą być przydatne do debugowania i rozwiązywania problemów z urządzeniem. Funkcje te nie wysyłają żadnych danych do Apple, o ile użytkownik nie stosuje dodatkowych narzędzi i wprost nie wyrazi na to zgody.

Przesyłanie danych między krajami

Apple współpracuje ze szkołami na całym świecie, aby tworzyć jak najlepsze narzędzia edukacyjne dla nauczycieli i uczniów.

Korzystanie z portalu Apple School Manager, nadzorowanych identyfikatorów Apple ID, iTunes U oraz iCloud może wiązać się z przechowywaniem danych osobowych poza krajem ich pochodzenia. Jednak niezależnie od miejsca przechowywania danych podlega zawsze tym samym rygorystycznym normom i wymaganiom.

Dane osobowe przesyłane w związku z działalnością Apple z Europejskiego Obszaru Gospodarczego lub Szwajcarii do Stanów Zjednoczonych Ameryki podlegają jednemu z aktywnych programów Safe Harbor lub programowi będącemu jego prawną kontynuacją, w którym Apple Inc. uczestniczy, na dowód czego posiada stosowny certyfikat, albo postanowieniom modelowym (Model Contractual Clauses)/szwajcarskiej umowie o transgranicznym przepływie danych (Swiss Transborder Data Flow Agreement) dołączonym/ dołączonej do Umowy o korzystanie z portalu Apple School Manager.

Dodatkowe materiały

Zaufanie ze strony szkoły i uczniów ma dla Apple pierwszorzędne znaczenie. Dlatego szanujemy prywatność uczniów i ją chronimy, przestrzegając rygorystycznych zasad postępowania z danymi.

Poniżej wymieniono dodatkowe materiały, w których można znaleźć więcej informacji na ten temat. Ponadto wszelkie pytania dotyczące ochrony prywatności można kierować do nas bezpośrednio ze strony www.apple.com/pl/privacy/contact.

Zasady ochrony prywatności obowiązujące w Apple: www.apple.com/pl/privacy/

Apple w edukacji: IT i wdrożenia www.apple.com/pl/education/it/

Umowa o korzystanie z portalu Apple School Manager: www.apple.com/legal/education/apple-school-manager/

Pomoc do portalu Apple School Manager: help.apple.com/schoolmanager/

Podręcznik wdrażania w sektorze edukacji: help.apple.com/deployment/education/

Podręcznik zabezpieczeń systemu iOS: www.apple.com/business/docs/iOS_Security_Guide.pdf



© 2016 Apple Inc. Wszelkie prawa zastrzeżone. Apple, logo Apple, Apple Pay, FaceTime, iMessage, iPad, iTunes U, Mac, Siri, Spotlight i Touch ID są znakami towarowymi Apple Inc. zastrzeżonymi w USA i innych krajach. HomeKit jest znakiem towarowym Apple Inc. iCloud i iTunes Store są znakami usług Apple Inc. zastrzeżonymi w USA i innych krajach. App Store jest znakiem usługi Apple Inc. IOS jest znakiem towarowym lub zastrzeżonym znakiem towarowym Cisco w USA i innych krajach, używanym na mocy licencji. Pozostałe nazwy przedsiębiorstw i produktów wymienione w niniejszym tekście mogą być znakami towarowymi odpowiednich podmiotów. Specyfikacje produktów mogą ulec zmianie bez powiadomienia. Maj 2016 r.