



Apple ve školství

Přehled zabezpečení dat a ochrany soukromí pro školy

Apple má školství ve své DNA. Technologie podle nás mají moc proměnit každou třídu a zaujmout každého studenta. Naše produkty jsou navrženy tak, aby šikovnými aplikacemi a poutavým obsahem na zařízeních, která učitelé i žáci baví používat, rozšiřovaly možnosti výuky a obohacovaly studium. Moc dobře víme, jak důležité je zabezpečení a ochrana dat, se kterými žáci při studiu pracují.

Zabezpečení a ochrana soukromí jsou fundamentálními atributy veškerého hardwaru, softwaru a služeb Apple. Náš integrovaný přístup zaručuje konzistentní zabezpečení a ochranu soukromí na všech úrovních uživatelské zkušenosti. Tento přístup počítá s ochranou soukromí a zabezpečením všech uživatelů ve školním prostředí včetně učitelů, zaměstnanců školy a studentů.

Některé funkce a služby jsme vytvořili přímo pro školství, například Apple School Manager, spravovaná Apple ID nebo Sdílený iPad. Tyto funkce jsou výsledkem toho samého integrovaného přístupu a berou v úvahu specifické bezpečnostní potřeby studentů a institucí.

Tento přehled rozebírá spravovaná Apple ID a to, jak naše související funkce a služby pro školství nakládají s daty a soukromím studentů. Můžete ho použít při komunikaci s rodiči o tom, jak Apple chrání data jejich dětí.

Apple a jeho závazek ochrany soukromí studentů

Apple nikdy nesleduje informace o studentech, nesdílí je ani je neprodává k reklamním nebo marketingovým účelům. Neprofilujeme studenty podle obsahu jejich e-mailů nebo podle jejich zvyklostí na webu. Stejně tak neshromažďujeme, nepoužíváme ani nikomu neposkytujeme osobní informace studentů za jiným účelem než kvůli poskytování vzdělávacích služeb. Apple neprodá informace o studentech ani je neposkytne za účelem cílení inzerce na studenty.

Apple svůj závazek dále potvrzuje svými [Zásadami ochrany soukromí](#) a [Smlouvou služby Apple School Manager](#), která definuje, jakým způsobem shromažďujeme, používáme, poskytujeme, přenášíme a uchováujeme informace uživatelů. Podepsali jsme rovněž [Slib ochrany soukromí studentů](#).

Apple School Manager a spravovaná Apple ID

Školám a institucím všech velikostí poskytuje Apple služby na usnadnění nasazení iPadů a Maců. Tyto služby byly vytvořeny s ohledem na zabezpečení a ochranu soukromí, aby data vaší instituce i studentů byla chráněna před implementací, v jejím průběhu i po jejím dokončení.

Apple School Manager je bezplatná webová služba, která poskytuje vše potřebné k nasazení iPadů a Maců ve školách. Apple School Manager umožňuje nakupovat obsah, konfigurovat automatickou registraci zařízení v systému na správu mobilních zařízení (MDM), vytvářet účty pro studenty a učitele a zakládat kurzy iTunes U.

Nejdůležitější funkcí Apple School Manageru je možnost vytvářet spravovaná Apple ID kontrolovaná institucí. Spravovaná Apple ID jsou nový typ Apple ID, který studentům umožňuje přistupovat k iCloudu, iTunes U a sdíleným iPadům a přitom nechává školám potřebný dohled a kontrolu. Spravovaná Apple ID jsou určena pouze pro využití ve školství.

Aby školy mohly studentům umožnit používat školní zařízení jen pro vzdělávací účely, jsou u spravovaných Apple ID některé vlastnosti a funkce zablokované. Studenti nemůžou nakupovat v App Storu, iBooks Storu nebo iTunes Storu. Deaktivované jsou taky funkce Apple Pay, Najít přátele, Najít iPhone, iCloud Mail, HomeKit a Klíčenka na iCloudu. Standardně jsou vypnuté i služby FaceTime a iMessage, avšak správce je může zapnout.

V nástroji Apple School Manager můžete automaticky vytvořit spravovaná Apple ID pro všechny své studenty a učitele, když nainportujete potřebná data ze školního informačního systému (SIS) nebo souboru CSV exportovaného ze školního adresáře. Každému uživateli se vytvoří účet na základě informací načtených ze zdroje. Další informace, například identifikátor spravovaného Apple ID a související heslo, se přidávají k informacím o účtu v Apple School Manageru. Zpátky do SIS se data nikdy nezapisují.

S každým účtem uživatele mohou být spojeny následující údaje, které se dají zobrazit v seznamu účtů nebo po výběru účtu:

- Jedinečný alfanumerický identifikátor daného účtu
- Křestní jméno, druhé jméno a příjmení
- Ročník, je-li zadán
- Zapsané hodiny
- E-mailová adresa, je-li zadána
- Role
- Místo
- Zdroj
- Datum vytvoření
- Datum úpravy

Protože spravovaná Apple ID vlastní a přiděluje vaše instituce, máte možnost snadno resetovat hesla, kontrolovat účty a definovat role pro všechny ve škole. Apple School Manager navíc protokoluje každou kontrolu účtu správcem nebo obnovení hesla, takže se o všech aktivitách uchovávají záznamy.

Spravovaná Apple ID podporují celou řadu variant přístupového kódu od jednoduchých čtyřciferných až po složité alfanumerické. Při prvotním importu nebo zakládání účtů generuje Apple School Manager dočasná hesla. Těmito dočasnými hesly se uživatelé ke spravovanému Apple ID přihlásí poprvé a potom musí každý uživatel své heslo změnit. Po změně dočasného hesla se už zvolené heslo studenta v Apple School Manageru nikdy nezobrazuje. Každý student se ke spravovanému Apple ID může přihlásit i ze zařízení, které nespravuje instituce, například aby mohl na zařízení doma dělat domácí úkoly. Při přihlašování ke spravovanému Apple ID musí kromě svého hesla zadat i šesticiferný ověřovací kód vygenerovaný administrátorem v Apple School Manageru. Tento dodatečný ověřovací kód po roce vyprší.

Apple School Manager může spravované Apple ID uvolnit, aby byl účet pro studenta, učitele, pracovníka školy nebo správce přístupný ještě zhruba 180 dní. Po jejich uplynutí se všechna data související s tímto účtem natrvalo smažou. Pokud instituce vyžádá okamžité smazání spravovaného Apple ID, přestane tento účet být přístupný a všechny s ním související informace se během 40 dnů natrvalo smažou.

Spravovaná Apple ID a sdílený iPad

Ve školách, kde studenti používají sdílené iPady, umožňuje Apple studentům přihlašovat se pomocí spravovaného Apple ID, aby se rychle dostali ke svým aplikacím, obsahu a nastavením. Na stejném iPadu se tak ke svému osobnímu učebnímu prostředí dostane několik studentů.

Při přihlašování studenta ke sdílenému iPadu se spravované Apple ID automaticky ověřuje na serverech identit Apple. Pokud student ještě dané zařízení nepoužil, vytvoří se mu nový domovský adresář a klíčenka. Po vytvoření a odemčení místního účtu uživatele se zařízení automaticky přihlásí k iCloudu. Vzápětí se obnoví nastavení daného studenta a jeho dokumenty a data se stáhnou z iCloudu.

Dokud je relace studenta aktivní a zařízení je připojené, dokumenty a data se při vytváření i úpravách ukládají na iCloud. Synchronizace na pozadí se navíc po odhlášení studenta postará o uložení všech změn na iCloud.

iCloud a zabezpečení dat

Pro studenty je při vytváření dokumentů, práci s lekcemi a aktivitách ve třídě důležité, aby svá data mohli bezpečně ukládat – na zařízení i v iCloudu.

Na iCloud se uživatelům automaticky ukládají nejen dokumenty, ale i kontakty, poznámky, záložky, události v kalendáři a připomínky. Ke všem svým informacím se dostanou z iOS i Macu a taky na webu [iCloud.com](https://www.icloud.com) – z Macu i PC. Jakmile se uživatel přihlásí k iCloudu, aplikace standardně získají přístup k iCloud Drivu. Přístup jednotlivých aplikací můžou uživatelé ovládat na panelu iCloud v Nastaveních. Výše uvedené služby jsou pro správu Apple ID standardně zapnuté.

iCloud používá standardní bezpečnostní mechanismy a přísné zásady ochrany dat. Uživatelská data šifruje před přenosem po internetu, na serverech je ukládá v zašifrovaném formátu a pro ověřování používá zabezpečené tokeny. To znamená, že data studentů jsou chráněna před neoprávněným přístupem jak při přenosu do zařízení, tak při uchovávání na iCloudu. iCloud používá minimálně 128bitové šifrování AES – stejnou úroveň zabezpečení jako přední finanční instituce – a nikdy neposkytuje šifrovací klíče žádným třetím stranám. Šifrovací klíče uchovává Apple ve svých vlastních datových centrech. Hesla a přihlašovací údaje studentů ukládá iCloud takovým způsobem, že k nim Apple nemá přístup pro čtení.

Další informace o zabezpečení iCloudu a ochraně soukromí najdete na stránce <https://support.apple.com/cs-cz/HT202303>.

CloudKit a aplikace jiných vývojářů

Aplikace jiných vývojářů jsou nedílnou součástí moderního studijního prostředí. Aby studenti mohli se svými daty stejně nekomplikovaně pracovat i v aplikacích jiných vývojářů, vytvořili jsme framework CloudKit, který mohou nezávislí vývojáři používat k ukládání a synchronizaci dat do iCloudu.

V aplikaci, která používá CloudKit, jsou studenti automaticky přihlášení svým Apple ID, takže si nemusí zakládat nový účet ani poskytovat jiné osobní informace. Vždycky se v takové aplikaci dostanou ke svým nejnovějším datům, aniž by si museli pamatovat další uživatelská jména nebo hesla. Vývojáři nemají přístup k Apple ID studentů, každého uživatele reprezentuje jen jedinečný identifikátor.

Bez ohledu na to, jestli vývojář používá CloudKit nebo ne, je důležité mít na paměti, že aplikace jiných vývojářů můžou o studentech shromažďovat data. Při používání aplikací jiných vývojářů je odpovědností vaší školy zajistit shodu se všemi platnými zákony. Vaše škola by měla posoudit podmínky, zásady a postupy aplikací jiných vývojářů, aby si udělala představu, jaká data můžou tyto aplikace od studentů shromažďovat, jak s nimi nakládají a zda není nutný souhlas rodičů.

V App Storu vyžaduje Apple od vývojářů souhlas s určitými pravidly, která mají chránit soukromí uživatelů a zabezpečení jejich dat. Pokud se dozvíme o aplikaci, která naše pravidla porušuje, musí vývojář problém napravit, jinak jeho aplikaci z App Storu odstraníme.

Polohové služby a režim ztráty

Studentům se při používání aplikací a služeb na zařízeních nejspíš zobrazí výzva k povolení polohových služeb pro určitou aplikaci nebo její aktivitu. Apple pro uživatele vytvořil granulární ovládací prvky, jimiž mohou spravovat sdílení polohových dat s aplikacemi a cloudovými službami.

Polohové služby umožňují aplikacím jako Mapy, Počasí nebo Fotoaparát přistupovat k datům o poloze a využívat je. Apple polohová data neshromažďuje ve formě, která by osobně identifikovala jednotlivé studenty. Polohové služby jsou standardně vypnuté, ale dají se zapnout jedním přepínačem v Nastaveních. A každou aplikaci, která požádá o přístup k polohovým datům, musí studenti schválit.

Když některá aplikace na iPadu používá polohové služby, zobrazuje se na stavovém řádku ikona šipky. Aplikace můžou požádat o to, aby k polohovým datům mohly přistupovat jen při používání anebo kdykoli. A je jen na uživateli, jestli takový přístup povolí; navíc svou volbu můžou v Nastaveních kdykoli změnit. Přístup se dá zcela zakázat, povolit při používání aplikace nebo povolit vždy. A pokud aplikace, kterým byl udělen přístup k informacím o poloze, toto oprávnění používají i na pozadí, zobrazí se uživateli po nějakém čase připomínka uděleného souhlasu. A můžou přístup aplikace podle svého uvážení změnit.

Polohové služby se používají i při hledání ztraceného nebo ukradeného zařízení. Na zařízení pod dohledem s iOS 9.3 nebo novějším může správce MDM na dálku aktivovat režim ztráty. Tím se aktuální uživatel odhlásí a zařízení se už nedá odemknout. Na obrazovce se zobrazí zpráva, kterou může správce upravit – třeba telefonní číslo, na kterém případný nálezců může zařízení nahlásit. Při aktivaci režimu ztráty může správce vyžádat, aby zařízení poslalo serveru MDM svou aktuální polohu. Když potom správce režim ztráty pro nalezené zařízení vypne, poloha zařízení se rovněž pošle a uživateli se zobrazí upozornění.

Diagnostická data

Pokud máte se svými studenty zájem přispět k dalšímu zdokonalování produktů a služeb Apple, můžete se přihlásit k účasti na našem programu diagnostiky a používání. Společnosti Apple se pak budou posílat neidentifikovatelné informace o vašich zařízeních a aplikacích.

Je to ovšem podmíněné explicitním souhlasem. Odesílaná data si uživatelé můžou na svém zařízení zobrazit a taky můžou jejich odesílání v Nastaveních kdykoli zastavit. V případě implementace sdílených iPadů může zasílání dat diagnostiky a používání zakázat škola.

iOS rovněž obsahuje vyspělé diagnostické funkce, které se mohou hodit při řešení potíží se zařízeními. Tyto vyspělé diagnostické funkce bez použití dalších nástrojů a explicitního souhlasu nepošílají žádná data společnosti Apple.

Mezinárodní přenosy dat

Apple spolupracuje se školami po celém světě, aby jejich učitelé měli k dispozici nejlepší nástroje.

Osobní data používaná v souvislosti se spravovanými Apple ID službami Apple School Manager, iTunes U a iCloud se mohou ukládat mimo zemi původu. Ať jsou uložena kdekoli, podléhají stejně přísným standardům a požadavkům.

Apple dbá na to, aby osobní data přenášená z Evropského hospodářského prostoru nebo Švýcarska do Spojených států amerických podléhala buď funkčnímu programu Safe Harbor či případnému nástupnickému programu, pro který je společnost Apple Inc. certifikována, anebo modelovým smluvním klauzulím / švýcarské dohodě o přeshraničním datovém toku, jež jsou připojeny ke Smlouvě služby Apple School Manager.

Další zdroje

Důvěra vaší školy a jejích studentů znamená pro Apple všechno. Proto respektuje soukromí studentů a chráníme ho přísnými pravidly, která určují, jak nakládáme s veškerými daty.

Další informace poskytují následující zdroje. Pokud máte ohledně ochrany soukromí jakékoli otázky, můžete se na nás vždycky obrátit přes stránku www.apple.com/privacy/contact.

Závazek společnosti Apple pro ochranu vašeho soukromí: www.apple.com/privacy/

Apple ve školství: IT a nasazení <http://www.apple.com/cz/education/it/>

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

Nápověda pro Apple School Manager: help.apple.com/schoolmanager/

Příručka k nasazení ve školství: help.apple.com/deployment/education/

Příručka k zabezpečení iOS: www.apple.com/business/docs/iOS_Security_Guide.pdf

