Læring med Apple
Oversigt over data og anonymitet til skoler

Indhold

I de sidste 40 år har Apples teknologi bidraget til at udvide grænserne for, hvordan lærere underviser, og elever lærer. Det er sket ved at give dem adgang til effektive værktøjer og apps, der kan skabe engagerende læringsoplevelser og slippe hver eneste elevs kreative potentiale løs. Vi er klar over, hvor vigtig sikkerhed og anonymitet er i forbindelse med beskyttelse af de data, eleverne producerer, gemmer og tilgår gennem hele undervisningsforløbet.

Sikkerhed og anonymitet er grundlæggende aspekter for udviklingen af alt Apples hardware, software og tjenester. Vores integrerede tilgang gør, at sikkerhed og anonymitet er indbygget i alle aspekter af læringsoplevelsen. Denne tilgang tager hensyn til alle brugernes sikkerhed og anonymitet, og det gælder også personer i et undervisningsmiljø såsom lærere, skolens personale og elever.

Vi har også udviklet funktioner og tjenester specifikt til undervisning, bl.a. Apple School Manager, administrerede Apple-id'er og Dele-iPad. Disse muligheder er skabt ved hjælp af selvsamme integrerede tilgang og med endnu større vægt på elevers og uddannelsesinstitutioners specifikke behov for sikkerhed og anonymitet.

Denne oversigt gennemgår, hvordan administrerede Apple-id'er og de tilknyttede undervisningsfunktioner og -tjenester håndterer elevdata og anonymitet. Oversigten kan bruges til at forklare forældre, hvordan Apple beskytter elevernes data.

Bemærk: Visse ordninger, tjenester, apps og bøger er ikke tilgængelige i alle lande. Sørg for at tjekke, hvad der findes i dit område.

Apples forpligtelse til at beskytte elevernes anonymitet

Apple hverken sporer, deler eller sælger elevdata til reklame- og markedsføringsformål. Vi bygger ikke elevprofiler ud fra indholdet i deres mails eller deres søgevaner på nettet. Ligeledes indsamler, bruger eller videregiver vi ikke elevernes personlige oplysninger til formål, der rækker ud over undervisning af eleverne. Apple vil hverken sælge elevernes personlige oplysninger eller videregive elevoplysninger med henblik på annoncering rettet mod eleverne.

For at uddybe vores forpligtelse har vi udarbejdet Apples anonymitetspolitik sammen med Apple School Manager-aftalen, der beskriver den måde, vi indsamler, bruger, videregiver, overfører og gemmer brugeroplysninger. Vi har derudover skrevet under på Student Privacy Pledge (forpligtelse over for elevers privatliv).

Apple School Manager og administrerede Apple id'er

Apple yder tjenester til skoler og institutioner af alle størrelser, så de nemt kan implementere iPad og Mac. Disse tjenester er udviklet med fokus på sikkerhed og anonymitet for at sikre, at institutionens og elevernes oplysninger er beskyttet før, under og efter implementeringen.

Apple School Manager er en gratis, webbaseret tjeneste, som har alt, hvad teknologiansvarlige skal bruge for at implementere iPad og Mac på deres skoler. Med Apple School Manager kan man købe indhold, konfigurere automatisk tilmelding af enheder i skolens løsning til administration af mobile enheder (MDM), oprette konti til elever og personale, oprette klasselister til Skolearbejde-appen og Klasseværelse-appen, aktivere registrering af elevernes fremskridt i Skolearbejde-appen samt administrere apps og bøger til undervisning og læring.

En central funktion ved Apple School Manager er muligheden for at lave administrerede Apple-id'er, som styres af institutionen. Administrerede Apple-id'er giver eleverne adgang til iCloud Drive, iCloud-fotobibliotek, Sikkerhedskopi, Skolearbejde og Dele-iPad, uden at skolen mister styringen. Administrerede Apple-id'er er kun udviklet til uddannelsesbrug.

For at sikre, at de enheder, som skoler deler ud til eleverne, kun bruges til undervisningsformål, har vi deaktiveret visse funktioner for administrerede Apple-id'er. Eleverne kan ikke købe noget i App Store, iBooks Store eller iTunes Store. Desuden er Apple Pay, Find mine venner, Find min iPhone, iCloud Mail, HomeKit og iCloud-nøglering alle deaktiveret. FaceTime og iMessage er som standard deaktiveret, men kan aktiveres af administratoren.

Med Apple School Manager kan man automatisk oprette administrerede Apple-id'er til alle elever og medarbejdere ved kun at importere de nødvendige data fra skolens elevdatasystem, enten direkte eller som CSV-filer fra skolens katalogtjeneste. Hver enkelt brugerkonto er oprettet med skrivebeskyttede oplysninger fra kilden. Ekstra oplysninger, f.eks. identifikatoren for det administrerede Apple-id og den tilknyttede adgangskode, føjes til kontooplysningerne i Apple School Manager. På intet tidspunkt skrives data tilbage til jeres elevdatasystem.

Følgende oplysninger kan være tilknyttet hver enkelt brugerkonto. Oplysninger kan ses på kontolisten eller ved at vælge en konto.

- Et alfanumerisk ID, der er unikt for kontoen
- Fornavn, mellemnavn og efternavn
- Klassetrin (hvis oplyst)
- Tilmeldte fag
- Mailadresse (hvis oplyst)
- Rolle
- Sted
- Kilde
- Oprettelsesdato
- Ændringsdato

Fordi skolen opretter og tildeler administrerede Apple-id'er, kan du nemt nulstille adgangskoder, inspicere konti og definere roller til alle på skolen. Hver gang, en konto bliver kontrolleret af en administrator, eller en adgangskode bliver nulstillet, registrerer Apple School Manager handlingen for at have en optegnelse over denne aktivitet.

Administrerede Apple-id'er understøtter også forskellige typer adgangskoder, lige fra avancerede kombinationer af bogstaver og tal til enkle firecifrede koder. Apple School Manager laver en midlertidig adgangskode til en konto, når den importeres eller oprettes første gang. Brugerne skal bruge den midlertidige adgangskode, første gang de logger ind på deres konto med deres administrerede Apple-id. Her skal brugerne ændre deres adgangskode. Så snart en elev ændrer den midlertidige adgangskode, viser Apple School Manager aldrig den nye adgangskode. Eleverne kan logge ind på en enhed, som ikke administreres af institutionen, for at få adgang til deres skolearbejde – f.eks. på en enhed hjemmefra. Det kan de gøre ved at logge ind med adgangskoden til deres administrerede Apple-id og en sekscifret bekræftelseskode, som administratoren tildeler den enkelte elev gennem Apple School Manager. Den ekstra bekræftelseskode udløber efter et år.

Når en institution sletter et administreret Apple-id, bliver alle oplysninger, der er tilknyttet denne brugerkonto, slettet fra Apples servere inden for 30 dage. Og når en skole ikke længere ønsker at bruge Apple School Manager, bliver alle elevdata slettet inden for 180 dage.

Skolearbejde

Skolearbejde-appen gør det nemmere for lærerne at dele undervisningsmateriale og få bedre indsigt i, hvordan eleverne gør fremskridt i de apps og bøger, lærerne vælger at bruge i undervisningen. Denne app bruger elevoplysninger og oplysninger fra klasselister, som administratorer har oprettet i Apple School Manager. Skolerne kan vælge at bruge Skolearbejde-appen til en særlig funktion – registrering af elevernes fremskridt – ved at aktivere den i Apple School Manager. Dermed kan app-udviklerne på en privat og sikker måde vise lærerne, hvor langt eleverne er kommet i forskellige aktiviteter, f.eks. når de skal læse et kapitel i en bog, løse en række matematikopgaver eller svare på spørgsmål i en quiz. Dette er kun muligt for aktiviteter tildelt i de miljøer, som skolen administrerer. De viste data gør det nemmere for både lærerne og eleverne at følge fremskridt i læringen for de tildelte aktiviteter, og lærerne kan bedre tilbyde yderligere aktiviteter eller ekstra hjælp ud fra de enkelte elevers behov.

Lærerne kan få vist forskellige oplysninger om fremskridt i aktiviteter, de har tildelt gennem Skolearbejde-appen, alt efter hvilken type data der genereres i den pågældende app. Det kan blandt andet være:

- Tidsforbrug
- Start- og sluttidspunkt
- Antal rigtige svar i en prøve
- Status for fremskridt
- Optjente point
- En af to værdier, f.eks. Ja/Nej, Sandt/Falsk, Færdig/Ikke færdig

Skolearbejde-appen er udviklet til at beskytte elevernes anonymitet. Når skolen aktiverer registrering af elevernes fremskridt i Apple School Manager, bliver der kun delt data om fremskridt for aktiviteter, som en lærer har tildelt direkte i form af et Handout gennem Skolearbejde-appen, og kun, når eleverne hver især bruger det administrerede Apple-id, som skolen har oprettet til dem, på deres enheder. Oplysninger om elevernes fremskridt i nogen anden aktivitet, der ikke er tildelt, bliver hverken delt eller vist. For eksempel: En lærer tildeler sin klasse den opgave, at de skal læse prologen til *Romeo og Julie* i iBooks, men en af eleverne er også i gang med at læse *The Great Gatsby*. Denne elev og læreren får kun vist data om fremskridt for prologen, fordi det var denne læseopgave, der blev tildelt. For at sikre gennemsigtighed, når rapportering af fremskridt er aktiveret, får eleverne vist en meddelelse om, at deres fremskridt registreres.

Klasseværelse

Med Klasseværelse-appen kan lærerne administrere elevernes iPad-enheder i klasselokalet, så de kan åbne apps og links på elevernes skærme for at hjælpe dem gennem en lektion. Lærerne kan nemt udveksle dokumenter med alle i klassen, og via funktionen Skærmoversigt kan de også se med på elevernes skærme for at holde øje med deres arbejde.

Klasseværelse kan kun bruges til at administrere elevernes iPad-enheder i løbet af lektionen, og der bliver ikke gemt nogen data, når lektionen er slut. Læreren og eleverne skal befinde sig tæt på hinanden, og de skal være logget på samme Wi-Fi-netværk og deltage i en aktiv lektion. Læreren kan kun administrere og se elevernes enheder under lektionen. For at sikre gennemsigtighed, når Skærmoversigt anvendes på en elevs skærm i klassen, vises der en meddelelse øverst på skærmen om, at læreren kigger med. Skoler kan også vælge at slå Skærmoversigt fra, hvis de ikke synes, at undervisere skal kunne se elevers skærme.

Administrerede Apple-id'er og Dele-iPad

I tilfælde, hvor elever deles om en iPad, giver Apple eleverne mulighed for at logge ind med et administreret Apple-id, så de hurtigt kan åbne og arbejde med deres egne apps, indhold og indstillinger. Det betyder, at flere elever kan deles om den samme iPad og stadig få en personlig læringsoplevelse.

Når en elev logger ind på Dele-iPad, kontrolleres det administrerede Apple-id automatisk med Apples identitetsservere. Hvis det er første gang eleven bruger enheden, vil en ny hjemmemappe og nøglering blive tildelt brugeren. Når elevens lokale konto er blevet oprettet og låst op, vil enheden automatisk logge ind på iCloud. Herefter gendannes elevens indstillinger, og elevens data og dokumenter synkroniseres fra iCloud.

Så længe eleven er logget ind på enheden, og enheden er tilkoblet, gemmes alle dokumenter og data i iCloud, når de oprettes eller ændres. Desuden sikrer synkronisering i baggrunden, at ændringer gemmes i iCloud, når eleven logger ud.

iCloud og datasikkerhed

Når eleverne laver dokumenter, interagerer med lektioner og deltager i aktiviteter i klasseværelset, er det vigtigt, at de kan gemme deres data, og at disse data altid er beskyttede – både på enheden og i iCloud.

Med iCloud kan eleverne automatisk gemme deres dokumenter, kontakter, noter, bogmærker, kalenderbegivenheder og påmindelser, så de har adgang til disse oplysninger på både iOS og Mac samt på iCloud.com på Mac eller PC. Administrerede Apple-id'er kan som standard bruge disse tjenester med 200 GB gratis iCloud-lagringsplads. Når en bruger logger ind på iCloud, får denne brugers apps adgang til iCloud Drive. Brugerne kan styre adgangskontrollen for hver app under iCloud i Indstillinger.

iCloud er bygget med sikkerhedsmetoder baseret på industristandarder og har strenge politikker omkring beskyttelse af data. iCloud beskytter brugerdata ved at kryptere dem, når de sendes over internettet, ved at lagre dem i et krypteret format, når de opbevares på serveren, og ved at bruge sikre koder til godkendelse. Elevdata er dermed beskyttet mod uautoriseret adgang, både under overførsel til enheder og ved lagring i iCloud. iCloud bruger som minimum 128-bit AES-kryptering – samme sikkerhedsniveau som i større finansielle institutioner – og giver aldrig krypteringsnøgler til tredjepart. Apple opbevarer krypteringsnøglerne i vores egne datacentre. iCloud gemmer også elevernes adgangskoder og brugeroplysninger på en sådan måde, at Apple hverken kan læse dem eller få adgang til dem.

Apple er ISO 27001- og 27018-certificeret for at have implementeret et system, der håndterer informationssikkerhed og beskytter personfølsomme oplysninger i offentligt tilgængelige cloud-systemer. Apples overholdelse af ISO-standarden blev certificeret af British Standards Institution. BSI's website indeholder overensstemmelsescertifikaterne for ISO 27001 og ISO 27018.

Der findes flere oplysninger her: Oversigt over sikkerheden i iCloud.

CloudKit og tredjepartsapps

Tredjepartsapps er en vigtig komponent i et moderne læringsmiljø. For at give eleverne den samme problemfrie oplevelse, når de gemmer og henter deres data i tredjepartsapps, har vi udviklet CloudKit – en platform, hvor tredjepartsudviklere kan gemme og synkronisere data til iCloud.

Eleverne bliver automatisk logget ind på de apps, der bruger CloudKit, med deres administrerede Apple-id. Det betyder, at de hverken behøver at oprette en ny konto eller angive andre personlige oplysninger. De vil altid have adgang til deres nyeste oplysninger i appen, uden at det er nødvendigt at huske nye brugernavne eller adgangskoder. Udviklere har ikke adgang til en elevs administrerede Apple-id – de har kun adgang til en unik identifikator.

Uanset om udvikleren bruger CloudKit eller ej, er det vigtigt at være opmærksom på, at tredjepartsapps muligvis indsamler data om eleven. Det er skolens ansvar, at alle relevante love og regler overholdes ved brug af

tredjepartsapps. Din skole bør gennemgå vilkår og betingelser, politikker og praksisser for tredjepartsapps for at blive klar over, hvilke data de eventuelt indsamler fra eleverne, hvordan disse data bruges, og hvorvidt dette kræver forældrenes samtykke.

I App Store kræver Apple, at app-udviklerne følger bestemte retningslinjer, der er udformet med henblik på at beskytte brugernes anonymitet og sikkerhed. Vi stiller nu også yderligere krav til alle udviklere, der anvender ClassKit, vores platform til registrering af elevernes fremskridt via Skolearbejde-appen. Ud over vores standardkrav til udgivelse af en app i App Store kræver vi, at udviklerne kun anvender ClassKit til formål, der er relevante for elevernes undervisning. Appen må ikke bruges til adfærdsbaseret annoncering, og udviklerne skal fremlægge en passende anonymitetspolitik for deres brug af data i enhver henseende.

Hvis vi bliver opmærksomme på en app, der er i modstrid med vores retningslinjer, skal udvikleren gøre noget ved problemet – ellers bliver appen fjernet fra App Store.

Lokalitetstjenester og funktionen Mistet

Når eleverne bruger apps og tjenester på deres enhed, vil de muligvis blive spurgt, om de vil slå Lokalitetstjenester til, afhængigt af den bestemte app eller aktivitet i appen. Apple giver brugerne detaljeret kontrol over, hvordan deres lokalitetsdata administreres og deles med apps og cloud-tjenester. Lokalitetstjenester er som standard slået fra, men eleverne kan slå denne funktion til igen, hvis skolen tillader det.

Apples lokalitetsbaserede, indbyggede apps, f.eks. Kort, Vejr og Kamera, skal anmode om tilladelse til at indsamle og bruge data, der angiver brugerens position. Når Apple indsamler disse lokalitetsoplysninger, sker det i en form, som ikke identificerer eleven personligt. Andre apps, som skolen stiller til rådighed, skal også anmode om tilladelse til at få adgang til lokalitetstjenester. Ligesom alle andre brugere af Apple-produkter kan eleverne godkende eller blokere adgang for hver app, der anmoder om at bruge tjenesten.

Adgangen kan indstilles til aldrig tilladt, kun tilladt når i brug eller altid, alt afhængig af appens anmodning om brug af lokalitet. Brugerne kan vælge at nægte adgang, og de kan når som helst ændre deres valg under Indstillinger. Desuden får brugerne en påmindelse, hvis en app gør brug af lokalitetsdata i baggrunden, også selvom brugerne tidligere har givet appen tilladelse til at bruge disse oplysninger. Brugerne kan så ændre adgangsindstillingerne for denne app, hvis de ønsker det. Når en app bruger Lokalitetstjenester, vises der en pil på menulinjen.

Skolen kan normalt ikke få adgang til en brugers position via Apples funktioner og tjenester. Lokalitetstjenester kan dog bruges til at hjælpe skolen med at finde en mistet eller stjålet enhed. På en enhed, der tilhører skolen, kan MDM-administratoren aktivere funktionen Mistet fra en ekstern placering. Når funktionen Mistet er aktiveret, logges den nuværende bruger af, og enheden kan ikke låses op. På skærmen vises der så en meddelelse, som administratoren kan tilpasse, f.eks. med et telefonnummer, man skal ringe til, hvis man finder enheden. Når funktionen Mistet er aktiveret på enheden, kan administratoren bede enheden om at sende dens aktuelle position tilbage til MDM-serveren. Når administratoren deaktiverer funktionen Mistet på enheden, sendes enhedens position ligeledes tilbage, og brugeren får besked om denne handling.

Oplysninger til analyseformål

Hvis du og dine elever vil hjælpe os med at forbedre Apples produkter og tjenester, kan du deltage i vores analyseprogram og sende oplysninger om jeres enheder, apps og programmer til Apple. Ingen af disse oplysninger er personligt identificerbare,

og det kræver dit udtrykkelige samtykke at gøre dette. Under Indstillinger kan brugerne til enhver tid se oplysningerne på deres enhed eller vælge, at de ikke længere vil sende disse data. Ved anvendelse af Dele-iPad kan skolen slå indsendelsen af analysedata fra via en begrænsning.

iOS har også avancerede diagnosticeringsfunktioner, som kan være nyttige til at udføre fejlfinding eller afhjælpe fejl på enheden. Disse funktioner sender ingen oplysninger til Apple, medmindre der bruges ekstra værktøjer og gives udtrykkeligt samtykke.

Dataoverførsel på verdensplan

Apple samarbejder med skoler i hele verden om at udstyre undervisere og klasseværelser med de bedste læringsværktøjer. For at understøtte brugen af Apple-tjenester samarbejder vi også med myndigheder om at sikre, at kravene til databehandling bliver opfyldt.

Med Apple School Manager, administrerede Apple-id'er og iCloud kan personlige data gemmes andre steder end hjemlandet. Uanset hvor disse data gemmes, gælder de samme strenge standarder og krav til lagring af data.

Apple sikrer, at personlige data, der overføres fra Det Europæiske Økonomiske Samarbejdsområde eller Schweiz til USA, er underlagt standardkontraktbestemmelser/en schweizisk aftale om datastrømme på tværs af landegrænser, som er godkendt af Europa-Kommissionen, eller enhver gældende Privacy Shield-certificeringsordning, som Apple Inc. måtte blive certificeret i henhold til. Standardkontraktbestemmelserne og den schweiziske aftale om datastrømme på tværs af landegrænser er vedlagt som bilag til Apple School Manager-aftalen.

Oversigt over anonymitet for forældre

Gennemsigtighed er en vigtig faktor for at kunne forstå, hvordan en elevs oplysninger bliver anvendt. Som en hjælp til at svare på eventuelle spørgsmål fra forældre eller værger har vi udarbejdet en oversigt over anonymitet for forældre. Vi opfordrer dig til at distribuere denne oversigt blandt alle med tilknytning til skolen for at forklare, hvordan elevoplysninger bliver indsamlet, anvendt og gemt, når skolerne bruger uddannelsestjenester og apps fra Apple.

Yderligere ressourcer

Hos Apple er din skoles og dine elevers tillid af afgørende betydning for os. Derfor respekterer vi elevernes anonymitet og beskytter den ved hjælp af stærk kryptering såvel som strenge politikker, der regulerer, hvordan alle data bliver håndteret.

Du kan få flere oplysninger i ressourcerne herunder, og hvis du har spørgsmål omkring anonymitet, kan du kontakte os direkte på www.apple.com/dk/privacy/contact.

- Om anonymitet og sikkerhed for Apple-produkter til uddannelse: https://support.apple.com/kb/HT208525
- Oversigt over anonymitet for forældre: https://images.apple.com/education/docs/Privacy_Overview_for_Parents.pdf
- Læring med Apple, IT og implementering: https://www.apple.com/dk/education/it/
- Apple School Manager-aftalen: https://www.apple.com/legal/education/apple-school-manager/
- Hjælp til Apple School Manager: https://help.apple.com/schoolmanager/
- Vejledning i implementering til uddannelsesinstitutioner: https://help.apple.com/deployment/education/
- Vejledningen iOS-sikkerhed: https://www.apple.com/dk/business/docs/iOS_Security_Guide.pdf
- Apples forpligtelse til at beskytte din anonymitet: https://www.apple.com/dk/privacy/