Sveriges Kommuner och Landsting

Avdelningen för digitalisering
2017-03-01

Vägledning, hantering av lärplattor i skolan

För att hantera lärplattor i skolan så smart och säkert som möjligt kan denna vägledning och checklista vara till hjälp. Vägledningen hör även samman med det stödmaterial[1] SKL tagit fram när det gäller användningen av molntjänster i skolan, eftersom det är viktigt att dokumentera och ha kontroll på informationshanteringen i de olika tjänsterna som används (hantering av personuppgifter, integritetsfrågor, informationssäkerhet etc.).

1. Bakgrund

Många skolverksamheter investerar i lärplattor[2] som digital enhet att använda för eleverna. Här har det tidigare varit en gråzon gällande hantering av användarkonton, lagring och inköp av appar. I den här vägledningen tar vi specifikt upp Apples produkt iPad och det nya avtal som kommit och som gör det lättare att göra rätt. I arbetet med att anpassa avtalet för svenska förhållanden har bl.a. jurister från Göteborg, Malmö och Stockholm varit engagerade.

Det finns också en checklista över saker att tänka på för att få till ett bra administreringsstöd för att hantera lärplattorna. Vägledningen och råden är med största sannolikhet tillämpbar på andra, liknande produkter och tjänster.

2. Molntjänster

Genom att välja en extern leverantör av en molntjänst, som ju en iPad med tillhörande Apple-id och möjlighet att lagra data i molnet (iCloud) är, kommer elever och pedagogers personuppgifter att behandlas av molntjänsteleverantören. Dessa molntjänster[3] är ofta standardiserade och villkoren för hur information kommer att hanteras av leverantören återfinns i omfattande standardavtal som kan vara komplicerade att förstå. Varje verksamhet som vill använda sådana tjänster måste se till att ha klart för sig vilka delar, tillägg och annat, som ingår i avtalet.

---

[1] http://skl.se/skolakulturfritid/skolaforskola/digitaliseringskola/molntjanster.96.html
[2] Begreppet lärplattor avser olika typer av enheter såsom iPads, smartphones och andra mobila enheter.
[3] Information om molntjänster finns även hos Pensionsmyndigheten som har tagit fram en rapport om molntjänster med en utförlig juridisk analys https://secure.pensionsmyndigheten.se/24304.html

Det kan vara svårt att ha full insyn i tjänsternas utformning och funktionalitet, men eftersom man har ansvar för vad som händer med personuppgifterna i tjänsten bör man anpassa vilken typ av information man väljer att hantera i standardiserade tjänster. Inom kommunerna har man ofta flera olika it-tjänster med olika möjligheter att lagra information och det är därför viktigt att ha riktlinjer och tydlighet gällande vad tjänsterna ska användas till och vilken information som lagras i vilka tjänster.

För skolverksamheter som använder eller vill använda denna typ av tjänster, kan SKL:s vägledning[4] fungera som stöd vid en bedömning av om den aktuella molntjänsten följer lagens krav och även kring den dokumentation som behövs.

3. Apples nya skolavtal

Juridiskt innebär Apples nya skolavtal[5] för användande av tjänsten ”Apple School Manager” bl.a. följande viktiga ändringar:

- Apple-kontot (Apple-ID) är personligt, men inte privat!
    - Det är skolhuvudman/skolan som har ansvar för kontot och att hanteringen sker enligt de svenska lagar och bestämmelser som finns (t.ex. vad gäller personuppgiftshantering, lagring, gallring)
    - Skolan tillhandahåller ett konto, ett s.k. hanterat Apple-ID, som blir personligt men avidentifierat, vilket innebär att samtycke inte behövs.
- Leverantören (Apple) får enbart hantera personuppgifter i enlighet med skolhuvudmannens instruktioner.
- Avtalet innehåller regleringar för insyn, gallring och underleverantörer som följer svensk lagstiftning.
- Avtalet innehåller också rätten till säkerhetsrevisioner, loggning etc.
- Apple har en godkänd ISO-certifiering gällande informationssäkerhet (ISO27001/2) och en gällande dokumenterat kvalitetsledningssystem som bl.a. säkerställer kundnytta, kundorientering och hantering av risker (ISO9001).

3.1. Tips – avtal och dokumentation

Precis som med övriga it-tjänster skolorna använder, behöver man som skolhuvudman ha koll på såväl avtal som dokumentation, i form av t.ex. PuL-bedömning och risk- och sårbarhetsanalys. Kommande Dataskyddsförordning[6] kommer att kräva att man kan visa upp att den här typen av analyser är genomförda, så säkerställ att analysen diarieförs.

Bedömningen ska alltid omfatta:

- En ***laglighetsbedömning***, dvs. om det sätt man vill behandla personuppgifter följer kraven i PuL samt
- En ***risk- och sårbarhetsanalys*** med avseende särskilt på personuppgiftsbehandlingen.

---

[4] http://skl.se/skolakulturfritid/skolaforskola/digitaliseringskola/molntjanster.96.html
[5] http://images.apple.com/legal/education/apple-school-manager/ASM-SE-EN.pdf
[6] Dataskyddsförordningen ersätter PuL i maj 2018, http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=SV

Idag måste personuppgiftsansvariga inför användning av en molntjänst genomföra och dokumentera analyserna. I kommande Dataskyddsförordning förändras rollerna något och även vem som ska ansvara och utföra arbetet, men oavsett så ska arbetet göras.

Till hjälp i arbetet finns bl.a. SKL:s vägledning för molntjänster som t.ex. innehåller mallar för PuL-bedömning och systemsäkerhetsanalys/risk- och sårbarhetsanalys (se fotnot 3).

4. Administrera lärplattor och distribuera appar

En administreringslösning, som ofta kallas MDM-tjänster (Mobile Device Management) är tjänster som gör det lättare att administrera och ha kontroll över de digitala enheter som finns i verksamheten, att registrera, konfigurera, koppla till användarens konto o.s.v. Används Apples enhetsregistreringsprogram (ERP) kan också själva registreringen av inköpta enheter ske automatiskt i MDM-tjänsten, vilket i princip innebär att ingen fysisk hantering och förberedelse av enheterna behövs innan användarna får dem.

När det gäller att välja MDM-lösning för sina lärplattor och/eller andra digitala enheter som används, finns det flera olika leverantörer att välja mellan. Det är en rörlig marknad, så att binda sig vid för långa avtal är inte att rekommendera alternativt bör man ha rimliga uppsägningstider så att man kan avsluta avtalet om så behövs.

Varför MDM (Mobile Device Management) och VPP (Volume Purchase Program)?

Genom att använda en MDM-lösning blir det enklare och säkrare att hantera lärplattorna som används i skolan. Varje lärplatta har ett Apple-ID som kopplas samman med det användarkonto eleven har i kommunen. När en elev slutar kan lärplattan installeras om och användas av någon annan istället. Blir lärplattan stulen kan man låsa den så att den inte går att använda, vilket gör den mindre stöldbegärlig. Det finns också möjlighet att använda funktionen ”hitta min iPad” för möjlighet att spåra lärplattan, men det är inte att rekommenderas då det kan bedömas som integritetskänsligt.

Det blir även enklare att distribuera och installera appar till de olika lärplattorna, vilket då kan göras via Apples VPP-lösning (Volume Purchase Program), där skolan/kommunen skapar ett konto. Apparna distribueras då inte via privata Apple-ID och licenserna kan återanvändas (appar kan hämtas tillbaka från en lärplatta och sedan delas ut på en annan). Inköpen som görs via VPP-lösningen kan registreras på respektive skola i MDM-tjänsten, där skolans administratör kan hålla koll (beroende på hur man har valt att delegera och lägga upp sin MDM-tjänst).

För själva betalningen av appar har Apple en lösning som kallas VPP-credit[7], men den fungerar för närvarande inte i Sverige (februari 2017). En lösning är att respektive skola/förskola har ett kreditkort, t.ex. Eurocard Purchasing Account eller liknande. En annan är att beställning och betalning av appar administreras centralt.

[7] https://support.apple.com/sv-se/HT202983

4.1. Tips – MDM och VPP

- Inventera
    - vilka sorts enheter ska administreras (enbart lärplattor eller även andra digitala enheter som används på skolorna/i kommunen)
    - vem ska kunna göra vad i administreringstjänsten
    - vilken utbildning behövs centralt och på respektive skola
- Delegera
  Diskutera på vilken nivå enheterna ska administreras och då t.ex. utifrån vad som kommer vara både effektivast och säkrast. Tänk på utmaningen att hitta rätt balans mellan flexibilitet och kraven på kompetens att göra rätt. Hur ska arbetet fungera över tid, vad är smartast på längre sikt? Diskutera för- och nackdelar med att administrera lärplattorna ute på skolorna respektive centralt. Kommunstorlek, antal enheter som ska administreras, hur resurser och kompetens ser ut idag, hur läromedelsinköp, support och service fungerar och är uppbyggt etc. är sådant som påverkar. Delegering skulle t.ex. innebära att:
    - lärplattorna läggs in i administreringstjänsten och kopplas till elevens inloggningsuppgifter av skolans utsedda resurs.
    - skolan kan organisera sina lärplattor så som det passar dem, för att t.ex. kunna distribuera appar på smidigt och ändamålsenligt sätt.
    - ledtiderna kan bli kortare, förutsatt att avsatt resurs finns på skolan och har tillräckligt med tid för uppdraget
    - varje skola ser och sköter sina egna inköp, har ansvar för sitt eget ”digitala läromedelsskåp”
    - utbildningsinsatser och avsatta resurser krävs ute på skolorna.
    - gemensamma riktlinjer och rutiner som följs upp för skolornas avsatta resurser behövs.
- Fysisk säkerhet
    - Se till att ha en tvingande låskod på enheterna och säkerställ rutiner för att kunna låsa läsplattan när den blir stulen, t ex genom MDM-verktyget
    - Stöldmärk med ”stöldmärkt och låst”.
    - Att låsa en stulen lärplatta går bl.a. genom aktiveringslåset som är en funktion i ”Hitta min iPhone” och som finns inbyggd i enheter med iOS 7 och senare. Man sätter enheten i ”förlorat läge” och kan på så vis förhindra återaktivering av borttappade eller stulna enheter. Som tidigare nämnt, kan just funktionen ”hitta min iPhone” vara integritetskänsligt och är, enligt Apples avtal, inaktiverad från start för alla hanterade Apple-ID:n. Äldre enheter kräver ytterligare inställningar för att de ska kunna låsas centralt ifrån.
- Informera och förankra
    - Dokumentera och informera om hur lärplattorna ska hanteras, framför allt vad som gäller vid köp och installation av appar, hantering av konton, vad som gäller vid stöld, förlorade eller förstörda enheter och ingångna avtal som lätt bara ”klickas i”.
    - Det är extra viktigt att informera om vad som gäller med lagring av information, t.ex. appar som lagrar personinformation eller information som är verksamhetskritisk och som behöver sparas jämfört med sådant som man kan ta bort utan att det gör något.
    - Ta fram riktlinjer kring var man ska spara vad, bserat på t.ex. PuL-bedömning och risk- och sårbarhetsanalys. Tydliggör vilken information användaren kan/får spara i iCloud respektive eventuella andra anvisade it-tjänster som finns i kommunen o.s.v.