

Riktlinjer för skydd av personuppgifter i grundskolan, fritidshem och förskolan

På Tankeborgen hanteras dagligen personuppgifter. Detta för att kunna utföra skolans uppdrag och ge eleverna det stöd de behöver. Även på huvudmannanivå utförs daglig personuppgiftshantering. För att kunna värna elevernas och vårdnadshavarnas rätt till integritet och trygghet ska rektor och varje medarbetare på vår skola – medvetet hantera personuppgifter enligt dessa riktlinjer.

Det som här sägs om grundskola gäller också fritidshem och förskola

Att tänka på:

- Dataskyddsförordningen är en rättighetslagstiftning som stärker individens rättigheter.
- Elevernas och vårdnadshavarnas personuppgifter är deras – vi lånar dem bara.
- Vi ska enbart använda de personuppgifter som vi verkligen behöver för det aktuella syftet.
- Vi ska i så liten utsträckning som möjligt hantera (samla in, lagra och sprida) känsliga personuppgifter.
- Vi ska i möjligaste mån eftersträva att vår hantering av personuppgifter vilar på annan rättslig grund än samtycke.

Personuppgiftsansvarig

För vår grundskola och förskola är det SSEK som är personuppgiftsansvarig för behandlingen av elevernas och vårdnadshavarnas personuppgifter. Det betyder att SSEK har det yttersta ansvaret för den personuppgiftsbehandling som sker för eleverna och deras vårdnadshavare vid Tankeborgen.

Digitala lärtjänster

Med digitala lärtjänster avses de olika webbaserade tjänster som används i undervisningen eller för att mäta elevernas kunskapsutveckling. Ett exempel på en digital lärtjänst är Skolpluss. För att trygga elevernas personuppgifter vid användning av dessa lärtjänster granskas och godkänns dessa av läraren. Godkända digitala lärtjänster finns på en rekommendationslista. Endast godkända tredjepartsappar får användas som en del i undervisningen.

Personuppgiftsincident

En personuppgiftsincident är en händelse där vi oavsiktligt förlorat, ändrat eller delat med oss av personuppgifter till någon obehörig. Exempel på personuppgiftsincidenter är när:

- ett mail med integritetskänsliga personuppgifter om en elev har skickats till fel person

När en personuppgiftsincident har inträffat ska rektor omgående informeras och incidenten ska anmälas. Rektor ansvarar för dokumentation och eventuell rapportering till Datainspektionen (inom 72 timmar från att incidenten identifierats). Vid behov informeras vårdnadshavare och elever om vad som skett och vilka åtgärder som vidtagits.

Att tänka på som medarbetare

Du ska till rektor anmäla alla former av personuppgiftsincidenter som du får kännedom om. Information till elev och/eller vårdnadshavare om en personuppgiftsincident ges av rektor.

Hantering av personuppgifter

Hantering av personuppgifter utgörs av flera olika moment där varje moment juridiskt sett betraktas som en personuppgiftsbehandling. Hanteringen av personuppgifter kan ses som en process som börjar med insamling och avslutas med gallring.

1. Informera

När personuppgifter ska behandlas, exempelvis när vårdnadshavare placerar sitt barn i kö eller när en elev börjar på skolan, måste vårdnadshavarna informeras om hur deras och barnets personuppgifter kommer att behandlas. Informationen ska lämnas innan personuppgifterna samlas in. Av informationen ska det bland annat framgå vem som är personuppgiftsansvarig, vilka personuppgifter som samlas in, den rättsliga grunden för att få hantera personuppgifterna, vad personuppgifterna ska användas till och hur länge de sparas. På Tankeborgen ges vårdnadshavarna och eleverna möjlighet till att ta del av denna information.

Att tänka på som rektor

- Du ansvarar för att vårdnadshavare i samband med att en elev börjar på skolan får information om hur personuppgifter hanteras .
- Du ansvarar för att årligen informera alla vårdnadshavare om varför och hur skolan hanterar deras barns och deras egna personuppgifter.
- Om det finns behov av att översätta informationen till ett annat språk, ta kontakt med tolk.

Grundskolans gemensamma text med information till vårdnadshavarna. Ska användas när vårdnadshavarna tackar ja till en plats samt årligen till alla.

2. Samtycka och registrera

Inför att personuppgifter samlas in måste en bedömning göras om huruvida ett samtycke krävs. I vilka situationer krävs ett samtycke? Se nedan för vägledning. Notera alltså att ett samtycke ska inhämtas innan skolan påbörjar insamling eller registrering av personuppgifter.

I grundskolan och förskolan krävs alltid båda vårdnadshavarnas samtycke:

- för att få publicera en bild eller film på sociala medier, på webbsida eller i tryck där barnet går att identifiera.
- om någon del av undervisningen sker på sociala medier där eleverna inte redan befinner sig. En förutsättning är att eleven och vårdnadshavaren uppfattar att det är frivilligt att samtycka.

Det är rektors ansvar att skolan har dokumenterade och korrekta samtycken för de situationer där bilder eller filmer används i skolans lokala marknadsföring. Rektor ansvarar också för att inaktuella samtycken gallras bort.

Ett samtycke kan återkallas om vårdnadshavarna är överens om det. Återkallande medför inte att den behandling som redan gjorts (exempelvis bildpubliceringar) blir olagliga. Däremot får vi inte fortsätta att använda personuppgifterna (exempelvis bilder) efter att samtycket återkallas.

Att tänka på som rektor

- Att samtycken sparas så att aktuella samtycken kan tas fram och inaktuella gallras ut.
- Att nya samtycken upprättas vid varje inskrivningsanmälan.

3. Spara

Att spara personuppgifter är detsamma som att lagra dem. Det finns olika alternativ; de kan lagras exempelvis i ett IT-system, i en molntjänst, i e-post, på en filserver, i ett USB-minne eller analogt i en pärm. Platsen för var personuppgifterna sparas måste väljas med omsorg och med insikt om hur skyddsvärda personuppgifterna är. De får inte sparas längre tid än vad som behövs för ändamålet.

Hur ska okänsliga personuppgifter sparas?

Okänsliga personuppgifter är harmlösa ur ett integritetsperspektiv och kan därför sparas digitalt på samtliga de lagringsplatser som till exempel på filservern, i e-post, i Google-drive/One-drive och i IT-system. Egna digitala system, utanför de uppräknade, är inte tillåtna.

Hur ska integritetskänsliga personuppgifter sparas?

Integritetskänsliga personuppgifter är exempelvis personnummer eller beskrivningar av studiesituationen, vilken kan innefatta såväl kunskapsutveckling som förutsättningar för den. Integritetskänsliga personuppgifter ska alltid hanteras med försiktighet och sparas i de system som är avsedda för syftet. Endast om hanteringen är säker kan sådan information exporteras ur systemet och sparas på annan plats.

Pedagogiska kartläggningar och utredningar kan sparas i Google-drive/One-drive så länge dokumentet delas enbart med den som har rätt till det, alternativt lokalt på datorn i ett lösenordsskyddat dokument.

Uppgifter om elevens och familjens sociala situation kan sparas i PMO, i Google-drive/One-drive så länge dokumentet delas enbart med den som har rätt till det, alternativt lokalt på datorn i ett lösenordsskyddat dokument.

Kränkingsanmälningar kan sparas i Google-drive/One-drive så länge dokumentet delas enbart med den som har rätt till det, alternativt lokalt på datorn i ett lösenordsskyddat dokument.

Tillbud/olycksfall kan sparas i Google-drive/One-drive så länge dokumentet delas enbart med den som har rätt till det, alternativt lokalt på datorn i ett lösenordsskyddat dokument.

Hur ska känsliga personuppgifter sparas?

Känsliga personuppgifter är uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning samt genetiska eller biometriska uppgifter. Känsliga personuppgifter ska alltid hanteras med extra försiktighet och sparas i avsedda IT-system. De ska inte lyftas ut ur avsedda IT-system eller sparas på annan plats om inte hanteringen är säker.

Elevhälsans lagstadgade kompetenser (skolpsykolog, skolläkare, skolsköterska, kurator och specialpedagogisk kompetens) ska spara sin dokumentation i PMO.

EHT-teamens dokumentation ska göras i PMO. Om tillgång till PMO saknas kan den sparas i Google Teamdrive/One-drive så länge dokumentet delas enbart med den som har rätt till det. Alternativt kan dokumentationen sparas lokalt på datorn i ett lösenordsskyddat dokument. Rektor är ansvarig för behörighetstilldelningen på Google Teamdrive/One-drive.

Personal i skolan kan behöva spara känsliga personuppgifter. Det kan exempelvis vara en lärare som behöver skriva egna minnesanteckningar för att alla elever utifrån sina behov ska få bästa förutsättningar. Denna typ av anteckningar kan sparas i Google-drive/One-drive så länge dokumentet delas enbart med den som har rätt till det, alternativt lokalt på datorn i ett lösenordsskyddat dokument.

Uppgifter om allergi och specialkost kan sparas i PMO, Google-drive/One-drive så länge dokumentet delas enbart med den som har rätt till det, alternativt lokalt på datorn i ett lösenordsskyddat dokument.

4. Dela

Med delning av personuppgifter avses att personuppgifter delas/sprids mellan individer. När person A delar personuppgifter med person B måste det göras med omsorg där det beaktas om det är okänsliga, integritetskänsliga eller känsliga personuppgifter som delas.

Hur ska okänsliga personuppgifter delas?

Okänsliga personuppgifter är harmlösa ur ett integritetsperspektiv och kan delas digitalt.

Hur ska integritetskänsliga personuppgifter delas?

Integritetskänsliga personuppgifter är exempelvis personnummer eller beskrivningar av studiesituationen vilken kan innefatta såväl kunskapsutveckling som förutsättningar för den. Om integritetskänsliga personuppgifter behöver delas utanför avsedda IT-system kan det göras på följande sätt:

- Via Google-drive/One-drive, där den som delar har kontroll över vem som får åtkomst och hur länge mottagaren ska ha åtkomst.
- Med ett krypterat och lösenordsskyddat USB-minne.

Hur ska känsliga personuppgifter delas?

Känsliga personuppgifter är uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning samt genetiska eller biometriska uppgifter. Om känsliga personuppgifter behöver delas utanför avsedda IT-system kan det göras på följande sätt:

- Via Google-drive/One-drive, där den som delar har kontroll över vem som får åtkomst och hur länge mottagaren ska ha åtkomst.
- Med krypterad e-post om filen är lösenordsskyddad och lösenordet skickas på annat sätt.
- Med ett krypterat och lösenordsskyddat USB-minne.

Registrering av frånvaro

Vid registrering av frånvaro får uppgifter om sjukdom eller hur eleven mår inte registreras. Enbart anmäld och oanmäld frånvaro får anges.

5. Arkivera/gallra

När ändamålet med personuppgifterna inte längre är aktuellt ska personuppgifterna gallras eller arkiveras. Huvudregeln är – om inget annat anges i arkiveringsrutinen – att personuppgifter om elever och vårdnadshavare ska gallras senast sex månader efter att eleven har slutat. Om särskilda skäl finns kan uppgifter sparas längre än sex månader. Ett exempel kan vara om det pågår en process, till exempel när en anmälan gjorts till Skolinspektionen, eller om en process kan förväntas. Varje rektor måste göra en bedömning av vilket material som behöver sparas under en längre tid och rektor ansvarar också för att uppgifter tas bort när de inte längre behövs.

Att tänka på

- personuppgifter måste gallras från samtliga platser som de lagras på, exempelvis e-post, filserver och pärmar

6. Dataskydd i specifika IT-system

Profdoc Medical Office (PMO)

Allmän beskrivning

Elevhälsan använder Profdoc Medical Office, PMO, vilket är ett elektroniskt dokumentationssystem som stödjer hanteringen av medicinska journaler, psykologiska journaler och ärendedokumentation i elevakten. PMO är CE-certifierat som en medicinteknisk produkt.

Elevhälsans medicinska insats erbjuder hälsobesök, vaccinationer och öppen mottagning som dokumenteras i den medicinska journalen. Elevhälsans medicinska insats tillämpar bestämmelsen om skyldighet att föra medicinsk patientjournal enligt patientdatalagen. Det innefattar dokumentation av personuppgifter och uppgifter om upplevelse av skolsituation och inläring, trivsel, kamratrelationer, hälsa, sjukdom, utveckling, inläringssvårigheter, matvanor, fysisk aktivitet samt social situation och vaccinationsstatus.

Elevhälsans psykologiska insats deltar generellt i elevhälsoarbetet och arbetar individuellt med elever på elevhälsans uppdrag. Individuella insatser genomförs och innefattar psykologutredningar (samtal, observationer, tester, frågeformulär) samt åtgärder utifrån de utredningar som genomförts. Elevhälsans psykologiska insats dokumenterar det utredande och åtgärdande arbetet i psykologisk patientjournal. Den psykologiska kompetensen tillämpar bestämmelsen om skyldighet att föra psykologisk patientjournal enligt patientdatalagen. Det innefattar dokumentation av personuppgifter och uppgifter som är relevanta i utredningar om upplevelse av skolsituation, inläring, testresultat, kamratrelationer, psykisk hälsa, utveckling, inläringssvårigheter, matvanor, fysisk aktivitet samt social situation och kontakter med andra vårdinstanser, liksom dokumentation av samtliga råd psykologen ger, överenskommelser med elev, pedagog, vårdnadshavare, insatser som psykologen utför och utvärdering av dessa insatser.

Elevhälsans psykosociala insats arbetar på uppdrag av elevhälsan men även individuellt. Kuratorn erbjuder såväl elever som vårdnadshavare besök, enskilt eller i grupp. Uppgifter om detta dokumenteras i kuratorsakten efter att elev/vårdnadshavare godkänt att anteckningar förs in i PMO. I elevakt dokumenteras alltid om elev eller vårdnadshavare varit i kontakt med kurator för att hela elevhälsan ska kunna följa ärendet och se att kontakt etablerats. I elevakt behöver kuratorn inte i detalj beskriva samtal som förts mellan elev och/eller vårdnadshavare och kurator, detta görs i kuratorsakt. Även utvärdering av insats dokumenteras i kuratorsakt/elevakt.

Elevhälsans specialpedagogiska kompetens – som företrädesvis är en specialpedagog eller speciallärare – deltar generellt i elevhälsoarbetet, stödjer lärare och undanröjer hinder i lärmiljöerna.

Specialpedagogisk kompetens använder elevakt i PMO för dokumentation av stödinsatser på skol-, grupp- och individnivå.

I elevakten dokumenteras

- utredning om elevs behov av särskilt stöd
- beslut om åtgärdsprogram
- utvärdering av åtgärdsprogram
- beslut att inte utarbeta åtgärdsprogram
- orosanmälan till socialtjänsten
- anmälan till rektor om upplevd kränkande behandling, omfattande frånvaro,
- särskilt stöd, olycksfall och annat
- utredning om upplevd kränkande behandling
- utredning om omfattande frånvaro
- handlingsplan vid kränkande behandling, omfattande frånvaro och socialt samspel
- anteckningar om observationer på klass- och individnivå
- skolpliktsanmälan till elevs hemkommun
- sammanfattade psykologutredningar (efter inhämtat samtycke från vårdnadshavare)

Åtkomst och behörighet

Elev och vårdnadshavare har inte åtkomst till dokumentationssystemet. Dokumentationssystemet tillämpar inte sammanhållen journalföring.

Behörighet att logga in i medicinsk journal har legitimerad sjuksköterska och legitimerad skolläkare. Tvåfaktorsautentisering tillämpas med SITHS-inloggning. Inloggningsuppgifterna är personliga och endast den som ”äger sitt inlogg” får använda det. Inloggningsuppgifterna får med andra ord inte lämnas ut till någon annan. Systematisk uppföljning sker av inloggningar, vilket innebär att den som öppnat en journal kan spåras. Eventuell åtkomst till en journal avgörs av vem användaren är, sekretessområdet, skolan och journaltypen, alltså i detta fall en medicinsk journal. En skolsköterskas eller en skolläkares åtkomst inaktiveras om personen i fråga slutar sin tjänstgöring. Då har skolsköterskan eller skolläkaren inte längre åtkomst till dokumentationssystemet.

Behörighet att logga in i psykologisk journal har enbart legitimerade psykologer som tillhör skolan, personal med systembehörighet och psykologisk verksamhetschef. Psykologisk verksamhetschef kontrollerar att inte otillbörlig användning sker.

Behörighet att logga in i kuratorsakt har kurator på skolan och systemansvariga.

Behörighet att logga in i elevakt har alla enligt skollagen lagstadgade kompetenser i elevhälsan: rektor som ledare av elevhälsan, specialpedagogisk kompetens (företrädesvis specialpedagog och speciallärare), skolsköterska, skolläkare, psykolog och kurator.