Anvisning informationssäkerhet

Denna anvisning har tagits fram för att vara ett stöd för myndighetens anställda i arbetet med att säkerställa att myndighetens informationssäkerhetsnivå upprätthålls. Anvisningen ger vägledning inom olika områden som berör känsligt material och som ska beaktas inom arbetet.

I denna anvisning tydliggörs ansvaret att skydda barns och ungas integritet och att skydda medarbetare och information mot olika former av risker och hot, såväl interna som externa.

Offentlighets- och sekretesslagen 33 kap. 2§

Sekretess gäller i verksamhet enligt lagen om Barnombudsman för uppgift om en enskilds personliga förhållanden, om inte det står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

För uppgift i en allmän handling gäller sekretessen högst i sjuttio år.

Omvänt skaderekvisit

Det så kallade omvända skaderekvisitet ovan utgår från sekretess som huvudregel. Också ett utlämnande av sådana uppgifter som vanligen inte är känsliga (till exempel en persons adress) kan ibland medföra risk för ”men”, till exempel om det kan antas att den som får uppgifterna skall använda dem för att utsätta den andre för våld eller trakasserier. Ordet ”men” betecknar i främsta rummet integritetskränkningar av olika slag som kan uppstå på grund av att uppgifter om en människas personliga förhållanden lämnas ut. ”Men” innefattar både kroppsliga ingrepp och psykiska obehag.

Ansvarsprincipen

Samtliga anställda ansvarar för att myndighetens informationssäkerhetsnivå upprätthålls. Det innebär främst att medarbetare ska planera och säkerställa att all information är skyddad enligt en fastställd klassificering av information.

Det handlar om att ta fram rutiner för att arbeta med skyddat material och riktlinjer för offentlig information.

Barnombudsmannen har arbetat utifrån principen att namn på barn, kommunikation med barn, transkriberingar, filmer, bilder och fotografier klassificeras som skyddat material. Det kan se annorlunda ut i din verksamhet beroende på vilket område det gäller.

Du behöver se över följande punkter:

- Hur förvarar vi personuppgifter och material som barnen har tagit fram?
- Hur transporterar vi arbetsmaterial, exempelvis minnesanteckningar, transkriberingar av samtal och digitala berättelser?
- Hur hanterar vi teknisk utrustning som används i våra träffar med barn? Exempelvis kameror, diktafoner, smartphones, surfplattor och USB-minnen.
- Behöver något material hanteras på särskilt sätt för att det innehåller känsliga uppgifter?

- Hur hanterar vi skyddade personuppgifter?
- Hur hanterar vi skriftliga godkännanden från vårdnadshavare?
- Hur hanterar vi mejlkorrespondens med barn och deras vårdnadshavare?
- Hur hanterar vi lokala hårddiskar, fristående hårddiskar och mappsystem i vårt datanätverk?
- Hur lagrar vi olika slags information som rör arbetet? Till exempel foton, anteckningar, inspelningar.
- Vem ansvarar för att allt material arkiveras och diarieförs i enlighet med framtagna rutiner?
- Vem ansvarar för att video, kamera och diktafon töms på material efter överföring till extern hårddisk?
- Vem ansvarar för att göra backup av material på en extern hårddisk som förvaras i ett brandsäkert skåp?
- Hur kommunicerar vi externt om arbetet, i vår telefonväxel och på webbplatsen?
- Vilka uppgifter lämnar vi ut när medarbetare reser för att träffa barn?
- Behöver vi använda fingerade namn i vår skriftliga dokumentation av arbetet? Då måste det finnas en förteckning över de barn som medverkat i arbetet för att kunna spåra dessa mot originalnamn.