Malmö stad

2025-08-11

Gymnasie- och vuxenutbildningsförvaltningen

Styrdokument

Dokumentets namn:
Riktlinjer gällande elever med skyddade personuppgifter i gymnasie- och vuxenutbildningsnämndens verksamheter

Typ av dokument:
Riktlinjer

Beslutad av:
Förvaltningens ledningsgrupp

Framtagen av:
Gymnasie- och vuxenutbildningsförvaltningen

Ansvarig chef:
Enhetschef digitalisering och IT

Ansvarig för uppföljning/revidering:
Enhetschef digitalisering och IT

Diarienummer:
GYVF-2025-1795

Version:
2

Datum för beslut:
2025-08-29

Organisation/område:
Gymnasie- och vuxenutbildningsförvaltningen

Reviderad:
2025

Följs upp:
Årligen

Riktlinjer gällande elever med skyddade personuppgifter i gymnasie- och vuxenutbildningsnämndens verksamheter

1. Inledning

Elever som riskerar att utsättas för hot eller våld kan få skyddade personuppgifter. Skyddade personuppgifter är Skatteverkets samlingsrubrik för de olika skyddsåtgärderna sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter. I skolans kontext innebär skyddade personuppgifter att en elev har någon form av särskilt skydd. Skydd i folkbokföringen innebär att personen har antingen skyddad folkbokföring eller en sekretessmarkering i folkbokföringsregistret. Sekretessmarkering syftar till att förhindra att elever med skyddade personuppgifter röjs och att elevens säkerhet äventyras. Enligt Skatteverkets vägledning för hantering av skyddade personuppgifter i svensk förvaltning (2020) ska varje myndighet ha egna riktlinjer för hur skyddade personuppgifter ska hanteras.

Detta dokument innehåller riktlinjer gällande skyddade personuppgifter för elever i all verksamhet inom Gymnasie- och vuxenutbildningsförvaltningen i Malmö stad. Syftet med riktlinjerna är att säkerställa att skyddade personuppgifter för elever hanteras på ett säkert sätt och att det samtidigt skapas en trygg och inkluderande skolsituation för elever.

Kommunala aktivitetsansvaret följer riktlinjens övergripande principer i framtagandet av sina egna rutiner.

Dessa riktlinjer omfattar inte vårdnadshavare, gymnasie- och vuxenutbildningsförvaltningens personal och elever som saknar uppehållstillstånd.

Riktlinjerna bygger på bestämmelserna i tryckfrihetsförordningen (TF 1949:105), offentlighets- och sekretesslagen (OSL 2009:400), dataskyddsförordningen (GDPR), folkbokföringslagen (FoL 1991:481), skollagen (SL 2010:800) samt Skatteverkets vägledning och övrig information om skyddade personuppgifter.

För att göra detta dokument mer lättläst görs följande förenkling i texten:

- ”Skola” syftar på all verksamhet inom förvaltningen.

1.1 Hantering av skyddade personuppgifter

För skyddade personuppgifter krävs extra försiktighet och tydliga rutiner. En säker hantering av dessa uppgifter bygger på:

- Tydliga rutiner som klargör hur personalen ska hantera skyddade personuppgifter i det dagliga arbetet.

- Begränsad åtkomst, vilket innebär att endast behörig personal får tillgång till de skyddade uppgifterna.
- Säkra IT-system som förhindrar obehörig åtkomst och läckage av känsliga uppgifter.
- Säkert informationsutbyte mellan myndigheter för att minimera risken för att skyddade uppgifter röjs.

Mer information och vägledning om hantering av skyddade personuppgifter finns på Skatteverkets webbplats.[1]

2. Skyddade personuppgifter och sekretess

2.1 Personuppgifter

Med personuppgifter menas all information som direkt eller indirekt kan hänföras till en levande fysisk person[2], exempelvis:

- Namn, personnummer
- Foto, e-postadress, adress, mobilnummer, ärendenummer, diarienummer, IP-adress, initialer
- Kombinationer av uppgifter, till exempel födelsedatum, klass eller adress
- Omdömen och värderingar
- Biometriska eller genetiska uppgifter

Vissa personuppgifter anses vara extra känsliga ur integritetssynpunkt, så kallade känsliga/särskilda personuppgifter.[3] Exempel på sådana känsliga personuppgifter är:

- Etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Hälsa

[1] Vägledning för offentliga aktörers hantering av skyddade personuppgifter | Skatteverket
[2] Artikel 4.1 i EU:s dataskyddsförordning.
[3] Artikel 9 i EU:s dataskyddsförordning; 3 kap. 1 § dataskyddslagen.

- Sexualliv och sexuell läggning
- Genetiska och biometriska uppgifter

Enligt EU:s dataskyddsförordning är utgångspunkten att känsliga personuppgifter inte får behandlas.[4] Undantag kan dock göras om behandlingen uppfyller vissa specifika villkor som föreskrivs i nationell rätt, antingen genom generell reglering 3 kap. 2–7 §§ kompletterande dataskyddslag[5], eller i sektorsspecifik reglering. Exempelvis får myndigheter vid behandling för viktiga allmänna intressen behandla känsliga personuppgifter om det krävs enligt lag, är nödvändigt för att handlägga ett ärende eller för att tillgodose ett viktigt allmänt intresse utan att innebära ett otillbörligt intrång i den registrerades integritet[6].[7] Exempelvis möjliggör detta undantag en behandling av känsliga personuppgifter i den mån det krävs för att kunna ta emot e-post eller diarieföra handlingar.[8] Känsliga personuppgifter kan även bevaras i arkiv eller samlas in för statistikändamål, men endast om samhällsnyttan tydligt överväger risken för att den enskildes integritet påverkas negativt.[9]

Med ”behandling av personuppgifter” menas all for av hantering som kan vidtas med en personuppgift (digital och analog).[10] Till exempel:

- Insamling
- Registrering
- Organisering, strukturering
- Lagring, bearbetning eller ändring
- Framtagning, läsning, användning
- Utlämning genom överföring, spridning eller tillhandahållande på annat sätt
- Justering eller sammanförande

---

[4] Artikel 9.1 i EU:s dataskyddsförordning.
[5] Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[6] För att avgöra om en behandling av känsliga personuppgifter innebär ett otillbörligt intrång måste myndigheten göra en avvägning mellan behovet av att behandla uppgifterna och den registrerades intresse av att skydda sin identitet. I denna bedömning ska läggas vikt vid bl.a. Uppgifternas känslighet, behandlingens karaktär och vilken spridning uppgifterna kan komma att få. Se prop. 2017/18:105 s. 194 f.
[7] 3 kap. 3 § dataskyddslagen.
[8] Prop. 2017/18:105 s. 194.
[9] 3 kap. 6–7 §§ dataskyddslagen.
[10] Artikel 4.2 i EU:s dataskyddsförordning

- Begränsning, gallring eller arkivering

2.2 Skyddade personuppgifter

Skyddade personuppgifter är Skatteverkets samlingsrubrik för de olika skyddsåtgärderna sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter. I detta sammanhang innebär skyddade personuppgifter att en elev har skydd i folkbokföringen.

Under vissa förutsättningar och efter ansökan hos Skatteverket kan en person få sina uppgifter i folkbokföringen skyddade genom att en sekretessmarkering registreras i folkbokföringsdatabasen. En sekretessmarkering är den lägre graden av skyddade personuppgifter. Det är en administrativ åtgärd som försvårar för andra att få tillgång till personens personuppgifter. Samtliga personuppgifter omfattas av sekretessmarkering. Skatteverkets sekretessmarkering är en varningssignal om att det alltid måste göras en noggrann sekretessprövning när någon begär att få ut en sekretessmarkerad uppgift (se avsnitt 2.3).

2.2.1 Skyddad folkbokföring

Skyddad folkbokföring ger ett starkare skydd än sekretessmarkering. När hotbilden mot en person är mycket stark kan personen få skyddsåtgärden skyddad folkbokföring av Skatteverket. Skyddad folkbokföring innebär att personen folkbokförs på en annan folkbokföringsort än där personen är bosatt. Någon bostadsadress registreras inte utan endast en boxadress till ett skattekontor. För att kunna få skyddad folkbokföring behöver personen flytta. Personen får även en markering för skyddad folkbokföring i folkbokföringsdatabasen, som följer med till kommunens skoladministrativa system. Sekretessen är stark för personuppgifter om den som har skyddad folkbokföring.

Sekretessen gäller både uppgifter som har aviserats av Skatteverket och som den enskilde själv har lämnat om dennes personliga förhållanden och uppgift som ensamt eller tillsammans med annan uppgift lämnar upplysning om var personen bor. Exempel på sådana uppgifter är personnummer, adress, e-postadress, telefonnummer, anhörig, skola med flera. Dessa uppgifter måste hanteras ytterst noggrant och normalt sett inte lämnas ut. Det måste vara helt klarlagt att ett utlämnande kan göras utan någon risk för den hotade och förföljda personen.

2.2.3 Fingerade personuppgifter

Personer utsatta för särskilt allvarlig brottslighet och som hotas till liv, hälsa eller frihet kan få fingerade personuppgifter genom ansökan vid polismyndigheten. Det innebär att personen får nya identitetsuppgifter, till exempel ett nytt namn och ett nytt personnummer via polismyndigheten. Vid fingerade personuppgifter tas den gamla identiteten bort helt från folkbokföringsregistret. Det innebär att skolan inte har kännedom om elever med fingerade personuppgifter.

2.3 Utlämnande av allmän handling innehållande personuppgifter

Enligt offentlighetsprincipen har alla rätt att ta del av allmänna handlingar eller uppgifter ur allmänna handlingar. Offentlighetsprincipen innebär att enskilda har rätt att ta del av handlingar som är förvarade hos en myndighet, som är inkomna eller upprättade där. Rätten att ta del av allmänna handlingar eller uppgifter får i vissa fall begränsas i lag. Det finns särskilda sekretessbestämmelser som innebär att en myndighet kan bedöma att en handling eller en uppgift ur en handling inte ska lämnas ut. Med sekretess menas ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av allmän handling eller på annat sätt (3 kap. 1 § OSL). Uppgifter som omfattas av sekretess ska maskeras innan myndigheten lämnar ut handlingen. En myndighet måste bedöma om det finns en relevant sekretessbestämmelse och därefter avgöra vilka uppgifter som kan och inte kan lämnas ut. Däremot kan det i vissa fall vara nödvändigt att bryta sekretessen och lämna ut en uppgift. Det framgår av de sekretessbrytande bestämmelserna i 10 kap. OSL.

2.3.1 Utlämnande till andra myndigheter/kommuner

Av 10 kap. 2 § OSL framgår att sekretessen kan brytas om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin egen verksamhet. Bestämmelsen är avsedd att tillämpas restriktivt och ger inte något generellt undantag för effektivitetsskäl. Det måste vara tydligt att utlämnandet krävs för att myndigheten själv ska kunna utföra sitt uppdrag.

En begäran om att få ta del av handlingar kan även inkomma från andra myndigheter. Vid en sådan begäran gäller, precis som ovan angetts, att en sekretessprövning måste göras och att det krävs att det finns en tillämplig sekretessbrytande bestämmelse för att uppgifterna ska kunna lämnas ut. Uppgifter kan alltså komma att lämnas till en annan myndighet enligt 10 kap. 27 § OSL, om det är uppenbart att intresset av att uppgiften lämnas ut väger

tyngre än det sekretessintresse som skyddas. Det handlar alltså om en intresseavvägning där behovet av uppgiften i den mottagande myndighetens verksamhet ställs mot risken för skada om uppgiften röjs.

En ytterligare möjlighet till utlämnande finns i 10 kap. 28 § OSL, där det anges att sekretess inte hindrar att en uppgift lämnas till en annan myndighet om uppgiftsskyldighet följer av lag eller förordning. Exempel på sådan uppgiftsskyldighet kan vara när en skola enligt lagen (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna. Om det inte finns någon uppgiftsskyldighet ska en prövning göras för att bedöma om det finns någon annan tillämplig sekretessbrytande bestämmelse. Finns det inte någon tillämplig sekretessbrytande bestämmelse kan uppgifterna inte lämnas ut. Begäran ska då hanteras på samma sätt som när enskilda begär att få ta del av handlingar. Om uppgifterna bedöms kunna lämnas ut ska utlämnandet ske på ett säkert sätt (rekommenderad post eller andra godkända kommunikationsvägar) som inte riskerar att röja uppgifterna för obehöriga.

Om uppgifter om en skyddad elev behöver begäras ut från en elevs tidigare hemkommun måste det säkerställas att elevens nuvarande hemkommun inte röjs. Som huvudregel ska vårdnadshavare eller myndig elev ombes att själv begära ut uppgifterna från den tidigare hemkommunen och få dem skickade med Skatteverkets postförmedlingsservice. För att uppgifterna ska kunna lämnas ut krävs även att en sekretessprövning görs.

2.3.2 Sekretessprövning vid skyddade personuppgifter

Skatteverkets sekretessmarkering ska ses som en varningssignal om att personen riskerar att utsättas för hot eller våld. En ny prövning ska göras i det enskilda fallet varje gång någon begär att få ta del av elevens personuppgifter. På Utbildningskontoret har vissa medarbetare som arbetar med elevstatistik och informationshantering tillgång till Skatteverkets verktyg Immer. Fråga närmsta chef om vem du ska vända dig till vid ett utlämnande för att säkerställa att skyddade personuppgifter inte lämnas ut.

För skolenheter säkerställs detta genom att använda barn- och elevregistret då det hämtar uppgifter om elever med skyddade personuppgifter från Immer.

När en medarbetare kontaktas med en begäran om att få ta del av uppgifter angående en elev med sekretessmarkering ska medarbetaren uppge att denne inte kan se att vi har några personuppgifter rörande eleven i våra system, att vi ska undersöka saken närmre och be att få återkomma.

Detta förfaringssätt ger tid för eftertanke och samråd med närmaste chef och/eller jurist om hur begäran ska hanteras och minimerar risken för att skyddade personuppgifter röjs.

Observera att skälet till att uppgifterna begärs ut inte ska efterfrågas. Personen som begär ut uppgifter har rätt att vara anonym, men att anonymiteten kan vara ett skäl till att det inte är möjligt att lämna ut uppgifter om en elev med skyddade personuppgifter.

2.3.4 Beslut om att inte lämna ut uppgifter

Om en medarbetare bedömer att en handling eller uppgift inte ska lämnas ut behöver medarbetaren upplysa den som har begärt att få ta del av handlingen om rätten att få ett skriftligt överklagbart beslut.

Rätten att meddela skriftligt beslut om att inte lämna ut allmänna handlingar eller uppgifter ur allmänna handlingar är delegerat till avdelningschef för hållbarhet och nämnd.

3. Hantering av skyddade personuppgifter i förvaltningens utbildningsverksamhet

3.1 Ansvar

Rektor samt övriga chefer ansvarar för att skyddade personuppgifter hanteras i enlighet med gällande författningar och dessa riktlinjer. Förvaltningschef ansvarar för att skyddade personuppgifter hanteras i enlighet med gällande författningar och dessa riktlinjer inom utbildningskontoret.
Rektor/förvaltningschef ansvarar för att all personal har kunskap om dessa riktlinjer samt att nyanställd personal och vikarier informeras.

Det är viktigt att elever med skyddade personuppgifter inte känner sig utpekade eller exkluderade. Så långt som möjligt ska därför skolans verksamhet anpassas så att alla elever kan delta. Samtidigt krävs ett kontinuerligt säkerhetstänkande kring elever med skyddade personuppgifter.

3.2. Personuppgiftssamordnare

Varje skolenhet ska ha en personuppgiftssamordnare utsedd av rektor. Små skolenheter kan ha en personuppgiftssamordnare gemensamt.

Personuppgiftssamordnaren ska ha kunskap om dessa riktlinjer och bistå rektor i arbetet kring elever med skyddade personuppgifter, exempelvis hantera handlingar och annan administration runt eleven samt informera nyanställda och vikarier. Det är även personuppgiftssamordnaren som ska se till att de

riktiga personuppgifterna till elever med skyddade personuppgifter finns att tillgå på skolan, samt att kontaktuppgifter till vårdnadshavare finns att tillgå i det fall eleven är under 18 år. I det fall att skolan själv får reda på att en elev fått skyddade personuppgifter ska skolan fråga eleven om vad hens riktiga personuppgifter är.

Övriga verksamheter inom förvaltningen behöver också följa gällande reglementen och riktlinjer om hantering av skyddade personuppgifter hos elever. Personuppgiftssamordnare för utbildningskontoret utgörs av dataskyddssamordnaren.

Vid byte av personuppgiftssamordnare ska rektor/ansvarig chef meddela detta till central samordnare på förvaltningen.

3.3 Ansökan och inskrivning

Ansökan till gymnasieskola, anpassad gymnasieskola och vuxenutbildning sker normalt via webb-ansökan. Har man skyddade personuppgifter ska ansökan göras på andra sätt för att kommunen ska kunna säkerställa sekretessen:

- Gymnasieskola, anpassad gymnasieskola: Ansökan görs via det digitala ansökningssystemet Dexter. Elevens ansökan registreras mot ett fiktivt personnummer och namn enligt styrdokumentet för Gymnasieantagning Skåne och västra Blekinge.
- Vuxenutbildning: Ansökan görs via ansökningsblankett hos mottagande funktion. På ansökningsblanketten uppges elevens riktiga namn och personnummer. Eleven ges ett TF-nummer och kan därefter söka kurser.

Efter att eleven har blivit antagen registreras eleven med fiktivt namn och personnummer som eleven väljer själv i det skoladministrativa verksamhetssystemet.

3.4 I väntan på skyddade personuppgifter

Om rektor får kännedom om att en elev ansökt om att få skyddade personuppgifter bör uppgifter om eleven hanteras med försiktighet. Rektor ansvarar över att personal som hanterar uppgifter om elever informeras. Eleven kommer att vara synlig i det elevadministrativa verksamhetssystemet och i andra IT-system till dess att Skatteverket har gett eleven skyddade personuppgifter.

Inga manuella ändringar får göras för eleven i IT-systemen i väntan på eventuellt skydd.

3.5 Dokumentation, diarieföring och arkivering

All dokumentation som rör elever med skyddade personuppgifter ska hanteras i enlighet med nämndens arkivredovisning och arkiveras enligt arkivlagen.

Om det kan antas att en uppgift i en allmän handling inte får lämnas ut på grund av en bestämmelse om sekretess, får myndigheten markera detta genom att en särskild anteckning (sekretessmarkering) görs på handlingen eller, om handlingen är elektronisk, införs i handlingen eller i det datasystem där den elektroniska handlingen hanteras. Anteckningen ska ange

1. tillämplig sekretessbestämmelse,
2. datum då anteckningen gjordes, och
3. den myndighet som har gjort anteckningen (5 kap. 5 § OSL).

När det gäller arkivering ska fysiska handlingar som kan hänföras till elever med skyddade personuppgifter förvaras separat från andra handlingar och vara inlåsta.

3.6 Tillgång till skyddade personuppgifter

För att minska risken att skyddade personuppgifter lämnas ut ska tillgången till skyddade personuppgifter begränsas till så få medarbetare som möjligt, både avseende tillgången till fysiska handlingar och tillgången i IT-system. Varje IT-system ska ha en rutin för behörighetstilldelning.

3.7 Skicka post till den som har skyddade personuppgifter

Post till personer med skyddade personuppgifter skickas via Skatteverkets postförmedlingsservice. Information om tillvägagångssätt finns på Skatteverkets webbplats.

3.8 Skyddade personuppgifter i IT-systemen

För att elever med skyddade personuppgifter ska kunna ta del av undervisning på samma sätt som andra kan det i skoladministrativa system ibland krävas att eleven förekommer med påhittade personuppgifter för att inte riskera att röja uppgifter till obehöriga.

Elever med skyddade personuppgifter får inte hanteras med sina riktiga uppgifter i ej krypterade IT-system. Uppgifter får heller inte föras över mellan system där överföringen sker utan kryptering. Individer med skyddade personuppgifter ska ej hänvisas till förvaltningens e-tjänster.

I barn- och elevregistret hämtas dagligen uppgifter från Skatteverket vilket möjliggör en snabb hantering av kontouppgifter i de fall en elev får skyddade

personuppgifter. Hantering av dessa elever sker främst av centralt placerade systemansvariga, men i de fall skolan först får kännedom om skyddade uppgifter ska detta meddelas till systemansvariga snarast. Tänk på att denna information inte ska skickas via mejl utan muntligt.

I syfte att inte röja känsliga personuppgifter kan det finnas behov av att elever med skyddade uppgifter hanteras på andra sätt än vad som är rutin, detta görs då i samråd med systemansvariga och verksamhet/skola.

3.8.1 Påhittade personuppgifter

Påhittade personuppgifter är inte detsamma som fingerade personuppgifter. Med påhittade personuppgifter menas här att elev med skyddade personuppgifter använder andra personuppgifter än de riktiga i skolans IT-system. Med påhittade personuppgifter möjliggörs användande av skolans IT-system, utan att elevens riktiga personuppgifter blir synliga eller sökbara.

Det är vårdnadshavare eller myndig elev som bestämmer vilket påhittat förnamn och efternamn som ska användas. Det ska vara ett fullständigt namn som används, dvs. både förnamn och efternamn. Både för- och efternamn ska ändras. Verksamheten bör se till att ett neutralt namn väljs, som inte riskerar röja eleven, vara utpekande eller iögonfallande.

3.8.2 När påhittade personuppgifter inte får användas

Påhittade personuppgifter får inte skrivas in i förvaltningens journal- och dokumentationssystem. Eleven ska vara registrerad med riktigt och fullständigt namn och personnummer i dessa system. Anledningen till detta är framför allt för att vi ska kunna garantera patientsäkerheten och att alla elever omfattas av journalhantering. Påhittade personuppgifter ska inte heller skrivas ut i diarieföringssystem, då informationen måste vara sökbar på längre sikt.

Vidare måste beslut som kan överklagas dokumenteras med elevens riktiga personuppgifter. Det gäller exempelvis beslut om mottagande, beslut om särskilt stöd/åtgärdsprogram samt vissa beslut om disciplinära åtgärder m fl. (se kapitel 28 i skollagen). Även interkommunala avtal måste upprättas med elevens riktiga personuppgifter.

Det kan också förekomma andra tillfällen då de riktiga personuppgifterna måste användas, exempelvis vid riskbedömning inför arbetsplatsförlagt lärande (APL).

3.8.3 Elevadministrativ system

Påhittade personuppgifter används i skoladministrativa system, dock anges alltid de korrekta personuppgifterna för att garantera en rättssäker myndighetsutövning, dvs. garantera att elever kan få ut sina betyg, samt för att uppfylla vår skyldighet att rapportera korrekta uppgifter, till exempelvis SCB och CSN.

3.8.4 Konto i IT-system

Elever med skyddade personuppgifter får ett konto till skolans alla IT-system, inklusive lärplattform, med påhittade personuppgifter.

3.8.5 Om skyddet upphör

När en elev blir av med en sekretessmarkering kommer konton att skapas med riktiga personuppgifter för denna elev automatiskt. Det kan komma att bildas dubbla konton, vilket systemadministratören hanterar. Det är personuppgiftssamordnaren som ska informera alla om att skyddet har upphört.

3.9 Intern överlämning av skyddade personuppgifter

Ska skyddade personuppgifter överlämnas mellan enheter/medarbetare ska de överlämnas personligen om inte annan säker överlämning kan garanteras. Antalet medarbetare som är inblandade i en överlämning ska minimeras och som huvudregel ska uppgifterna lämnas direkt till den medarbetare som är avsedd mottagare.

3.10 Hantering av skyddade personuppgifter i övrigt

Personuppgifter används i många sammanhang inom kommunen, utöver i kommunens IT-system. Exempel på situationer där personuppgifter hanteras är vid skolskjuts, resebidrag/busskort, skol-ID, fotokatalog, specialkost, fakturering, utbetalning av elevpeng, kommunalt aktivitetsansvar, med mera. Det är viktigt att begränsa spridningen av skyddade personuppgifter. Generellt ska skyddade personuppgifter hanteras manuellt istället för elektroniskt, om IT- säkerheten inte kan garanteras. Fler personuppgifter än nödvändigt ska inte användas. Exempelvis ska inte efternamn och personnummer användas om det räcker med förnamn. Det är rektor/chef för enheten och förvaltningschef som ansvarar för att kontinuerligt se över hanteringen av skyddade personuppgifter samt att vid behov upprätta lokala rutiner för hantering av skyddade personuppgifter.

3.11 Om skyddade personuppgifter lämnas ut av misstag

Om skyddade personuppgifter lämnas ut av misstag, agera i enlighet med kommunens rutin för personuppgiftsincidenter.

Rektor, personuppgiftssamordnare samt vårdnadshavare ska informeras om att personuppgifterna har lämnats ut.

Rektor ska skyndsamt kontakta förvaltningens dataskyddssamordnare för att dokumentera incidenten. Det inträffade kan bedömas vara så pass allvarligt att det ska anmälas vidare till Integritetsskyddsmyndigheten, vilket ska ske inom 72 timmar från upptäckten av incidenten.