TJÄNSTESKRIVELSE

Datum
2022-01-05
Diarienummer
FG 2021-01049

Kungsbacka

Regelbunden granskning hösten 2021 - dataskyddsområdet

Förslag till beslut i nämnden för Förskola & Grundskola

Nämnden har tagit del av informationen och lägger denna till handlingarna.

Sammanfattning av ärendet

Enligt dataskyddsförordningen ska varje myndighet utse ett dataskyddsombud. Dataskyddsombudet har uppsikt över verksamhetens efterlevnad av dataskyddsreglerna som syftar till att värna den enskildes integritet. Därför har kommunens gemensamma dataskyddsombud under hösten genomfört en granskning av respektive nämnds och bolags dataskyddsarbete i stort. Det övergripande syftet för granskningen är att stimulera till reflektion och lärande omkring den egna verksamhetens dataskyddskapacitet. Med utgångpunkt i granskningen ges råd och rekommendationer som dels kan bidra till att bibehålla och stärka dataskyddet i verksamheten, dels omhänderta eventuella avvikelser. Ett aktivt dataskyddsarbete innebär en stor trygghet för dem vars personuppgifter som verksamheten hanterar.

Resultatet av granskningen av nämnden för Förskola & Grundskola visar på att nämnden i allt väsentligt möter de övergripande kraven inom merparten av de granskade områdena. Inom de områden där det finns utvecklingsområden är detta känt på förvaltningen. Dataskyddsombudet lämnar i rapporten rekommendationer om vilka områden det behövs åtgärder.

Beslutsunderlag

FG Myndighet & Stöds tjänsteskrivelse, 2021-01-04

Dataskyddsombudets rapport efter regelbunden granskning 2021, 2021-12-01

Beslutet skickas till

-

Maria Andersson
Förvaltningschef

Frida Byrsten
Verksamhetschef Myndighet & Stöd

FG Myndighet & Stöd

Frida Byrsten
070-265 59 66
Verksamhetschef

Kungsbacka kommun
434 81 Kungsbacka

Besöksadress
Stadshuset, Storgatan 37

Telefon 0300-83 40 00

www.kungsbacka.se

Datum
2021-12-01

Nämnden för Förskola & Grundskola
forskola.grundskola@kungsbacka.se

Kungsbacka

Dataskyddsombudets rapport efter regelbunden granskning 2021

Verksamhet som granskningen rör: Nämnden för Förskola & Grundskola

Granskningens omfång: Granskningen omfattar områdena *Organisering, Koll på personuppgiftsbehandlingen, Säker behandling, Registrerades rättigheter*, *Utkontraktering och gemensamt personuppgiftsansvar* samt *Systematiskt kvalitetssäkringsarbete*. Se bilaga 1 för mer information om granskningen.

Granskning gjord av: Karin Malmsten, dataskyddsombud

Granskningens diarienummer: KS 2021-00863

Uppföljning: Åtgärderna som vidtas för att omhänderta granskningens resultat kommer att ingå i nästkommande regelbundna granskning hösten 2022.

Granskningens resultat

Det har av granskningen inte framkommit annat än att nämnden för Förskola & Grundskola i allt väsentligt möter de övergripande kraven inom flera av de granskade områdena.

En bidragande faktor till detta bedömer jag är att verksamheten har kompetenta krafter och resurser inom både lednings- och stödorganisationen som samverkar inom och utanför nämndens ansvarsområde och har en god insikt om verksamhetens risker och utvecklingsbehov.

Min granskning bekräftar vad verksamheten själv identifierat som styrke- respektive utvecklingsområden i sina genomgångar av dataskyddet, men visar också på sådant som inte ännu har omhändertagits. Avvikelser har genom granskningen visats inom följande områden och punkter, vilka jag rekommenderar nämnden för Förskola & Grundskola att omhänderta.

Granskningen visar följande

I tabellen nedan framgår de områden och tillhörande granskningspunkter som ingått i granskningen. De aspekter som granskningen funnit avvikelser inom är markerade med röd eller orange färg. Röd färg anger att det av granskningen framkommit att det förekommer avvikelser i sin helhet, medan orange färg anger att avvikelse förekommer delvis. Grön färg anger att det av granskningen inte framkommit avvikelser i nämnvärd utsträckning.

Nr	Granskningspunkter	Förordnings- eller policysstöd[1]
Organisering		
1	Ansvarsfördelningen för dataskyddsarbetet i verksamheten är dokumenterad och känd.	Art. 4.7, art. 24
2	Det finns en utsedd dataskyddskontakt som arbetar löpande med samordningen av dataskyddet i verksamheten.	KS Riktlinjer för hantering av personuppgifter (2018-05-29 §147), punkt 2.
3	Det finns samverkande funktioner med bred kompetens som tillsammans driver och förankrar dataskyddsarbetet.	Art. 25.1-2
Koll på personuppgiftsbehandlingen		
4	Registret över verksamhetens personuppgiftsbehandlingar är komplett och behandlingarna har försetts med lämpliga skyddsåtgärder.	Art. 30.1 a–g; art. 32
Kommentar Nämndens personuppgiftsbehandlingar är identifierade och utförligt förtecknade i ett behandlingsregister. Av förteckningen framgår också att skyddsåtgärderna varierar i omfattning för de olika behandlingarna vilket visar på att nämnden avgjort lämplig säkerhet på behandlingsnivå. Samtidigt noterar jag att verksamheten själv har identifierat och adresserat ytterligare anpassningsbehov både i den tekniska säkerheten, såsom tillräcklig autentisering, och i den organisatoriska säkerheten, såsom utökade behörighetsrutiner. Med utgångspunkt i verksamhetens personuppgiftsbehandling och dess registreradegrupper rekommenderar jag nämnden att fortsätta och fullfölja detta arbete för att uppnå en tillräcklig skyddsnivå i sin personuppgiftsbehandling enligt art. 32.		
5	Konsekvensbedömning görs för riskbehandlingar.	Art. 35.1-11 samt art. 36.1
Bedömning Jag konstaterar att nämnden har identifierat sina riskbehandlingar och genomfört konsekvensbedömning för flera av dessa. För övriga har en prioritetsordning gjorts där analys inletts dels för behandlingar som har koppling till tredjeland, dels för behandlingar som i någon del genomförs som e-tjänst för verksamheternas externa målgrupper. Ännu har dock inte alla riskbehandlingar inom nämndens verksamhetsområde omhändertagits genom tröskelanalys och konsekvensbedömning enligt art. 35.		

[1] För den verksamhet som omfattas av brottsdatalagen tillämpas istället motsvarande lagrum i brottsdatalagen (2018:1177)

Förslag till åtgärd

Genomför tröskelanalys för samtliga riskbehandlingar inom nämndens ansvarsområde samt efterföljande konsekvensbedömning för de behandlingar där det visar sig behövas. Flera behandlingar av samma art kan med fördel omhändertas i samma konsekvensbedömning och genomföras i samverkan med andra nämnder som utför liknande behandling i sin verksamhet.

Säker behandling		
6	Instruktioner finns tillgängliga för personalen om hur de ska handskas med personuppgifter i det dagliga arbetet.	Art. 25.1-2
7	Dataskyddsfrågor diskuteras regelbundet i verksamheten, exempelvis i samband med APT och enhets-/avdelningsmöten.	Art. 25.1-2
8	Det finns rutiner för hur personuppgiftsincidenter ska upptäckas, rapporteras och tas omhand.	Art. 33-34
Registrerades rättigheter		
9	De registrerade informeras om hur deras personuppgifter behandlas i verksamheten.	Art. 5.1 a, art. 12. 1-2 (inbegripet art. 13-14)

Bedömning

Information om nämndens personuppgiftsbehandling ges till registrerade dels genom en generell information om personuppgiftsbehandling i Kungsbacka kommun på dess hemsida samt en utförlig verksamhetsspecifik information på Förskola & Grundskolas egna sidor på kungsbacka.se. Dels ges utförlig information även i samband med insamlande av uppgifter genom till exempel e-tjänster. Informationen som ges är också skriven på ett i huvudsak enkelt och begripligt sätt. Därmed motsvarar informationen som nämnden ger till de registrerade i allt väsentligt de övergripande krav som GDPR ställer på den personuppgiftsansvariges informationsplikt.

Dock ges ingen information om förekomsten av och säkerheten vid behandling som innebär att uppgifter överförs till tredjeland inom nämndens område, vilket innebär en avvikelse mot art. 13.1 f och 14.1 f.

Förslag till åtgärd

Komplettera informationen till de registrerade med de upplysningar som ska lämnas enligt art. 13.1 f när personuppgifter samlas in direkt från de registrerade, och i förekommande fall 14.1 f när uppgifter samlas in på annat sätt.

Övrigt

Trots utförlig information om nämndens personuppgiftsbehandling i övrigt finns anledning att överväga att ta fram och tillgängliggöra en ännu mer elevnära information som riktar sig till de barn och unga som medverkar i nämndens verksamhet. Detta som ett led i att säkerställa öppenheten i behandlingen enligt art. 5.1 a samt 12.1 och med beaktande av barnkonventionen för att underlätta för barn under 18 år att tillvarata sin rätt till information om hur deras personuppgifter behandlas i samband med deras utbildning.

För kännedom har jag det av granskningen framkommit att kommunens standardiserade e-postsignatur saknas information i samband med insamlingen av personuppgifter som sker i detta sammanhang, vilket avviker mot art. 13.1-2. Detta har jag hänfört till kommunstyrelsen att omhänderta inom ramen för sin samordnande roll vad gäller kommunens övergripande kommunikation.

10	De registrerade informeras om rättigheterna de har.	Art. 13.2 b-d, art. 14.2 c-e
Kommentar Trots en i huvudsak tydlig och utförlig information till de registrerade om deras rättigheter på kommunens hemsida finns anledning att överväga att ta fram och tillgängliggöra en ännu mer elevnära information som riktar sig till barn och unga som medverkar i nämndens verksamhet. Detta som ett led i att säkerställa öppenheten i behandlingen enligt art. 5.1 a samt 12.1 och med beaktande av barnkonventionen för att underlätta för barn under 18 år att tillvarata sina rättigheter på personuppgiftsområdet.		
11	Det finns rutiner för att ta emot, hantera och besluta om de rättigheter som de registrerade kan åberopa[2].	Art. 15 -21
Utkontraktering och gemensamt personuppgiftsansvar		
12	Det finns rutiner för att krav som rör dataskydd ingår vid upphandling av digitala verksamhetssystem och tjänster.	Art. 28
Kommentar För kännedom har det av granskningen framkommit att det finns behov att förtydliga den kommunövergripande metod- och processbeskrivningen för upphandling av digitala verksamhetssystem och tjänster som inbegriper personuppgifter. Detta så att endast biträden som lämnar tillräckliga garantier om dataskydd enligt GDPR anlitas för kommunens och dess nämnders räkning enligt art. 28.1. Detta har jag hänfört till nämnden för Service som ägare för kommunens övergripande upphandlingsmetodik.		
13	Det finns aktuella avtal med de personuppgiftsbiträden som verksamheten anlitat eller är gemensamt ansvariga tillsammans med.	Art. 28, art. 26
Kommentar Det finns aktuella arrangemang för behandlingssituationer där nämnden för Förskola & Grundskola är gemensamt personuppgiftsansvarig tillsammans med en annan verksamhet, exempelvis för kamerabevakning i utbildningslokalerna. Jag rekommenderar dock att tydliggöra i informationen till de registrerade (på både hemsida och genom skyltning i lokalerna) att det föreligger ett gemensamt personuppgiftsansvar och mellan vilka så att det blir helt tydligt i linje med intentionerna i art. 26.2. Där anges att det väsentliga innehållet i arrangemanget ska göras tillgängligt för de registrerade. I Integritetsskyddsmyndighetens vägledning för kamerabevakning (IMY rapport 2021:2) finns exempel på utformning av skyltning.		
Systematiskt kvalitetssäkringsarbete		
14	Det finns arbetssätt för egenkontroll på dataskyddsområdet, som följs upp av verksamhetens ledning och nämnd/styrelse.	Art. 5.2
15	Verksamheten har utnämnt och anmält dataskyddsombud till IMY.	Art. 37

Övergripande rekommendation och uppföljning

Min granskning har visat ett antal avvikelser och jag rekommenderar nämnden att omhänderta dessa för att stärka dataskyddet för de registrerade. Ju förr det kan göras desto bättre är det ur ett registreradeperspektiv. Uppföljning kommer göras i samband med 2022 års regelbundna granskning. Dessförinnan erbjuder jag uppföljning inom ramen för råd och stöd. Nämnden kan själv

[2] Rätt till radering, återkallade av samtycke, rättelse, flytt av personuppgifter, invända mot behandling eller begära begränsning samt klaga på behandling.

påkalla en särskild uppföljning för att få en oberoende bedömning av sitt utvecklingsarbete inom de aktuella avvikelseområdena.

Det står förstås nämnden fritt att avgöra hur avvikelserna ska omhändertas men förslag till åtgärder ges i samband med varje enskild avvikelse. Därutöver bedömer jag att en god idé är att överväga att stärka handlingsutrymmet för de kunniga och skickliga medarbetare som finns i verksamheten. Detta då orsakerna till avvikelserna synes härröra från tidsbrist snarare än bristande kompetens. Ledningens uppföljning och genomgång av effekterna av förstärkningen är också väsentlig så att förstärkningen ytterst kommer de registrerade till del.

Kungsbacka 2021-12-01

Karin Malmsten

Dataskyddsombud

Bilaga 1: Om granskningen

En del av dataskyddsombudets uppdrag

Av art. 39 i dataskyddsförordningen framgår att jag som dataskyddsombud ska ha uppsikt över efterlevnaden av GDPR, de svenska kompletterande dataskyddsbestämmelserna samt den personuppgiftsansvariges strategi för skydd av personuppgifter. En del av detta arbete gör jag genom att granska respektive nämnds/bolags/stiftelses följsamhet mot GDPR och rapportera avvikelser som jag uppmärksammar. I mitt uppdrag ingår att ta vederbörlig hänsyn till de risker som är förknippade med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften.

Den planerade granskningen för perioden 2021-2022 omfattar *regelbunden granskning* och *fördjupad granskning*. Den regelbundna granskningen omfattar samtliga personuppgiftsansvariga verksamheter i kommunen och är inriktad på verksamheternas dataskyddsarbete i stort[3], medan den fördjupade granskningen görs inom ett avgränsat område som inte per automatik omfattar samtliga verksamheter. Den regelbundna granskningen görs på hösten och den fördjupade granskningen görs på våren. Därutöver finns utrymme för riktad granskning närhelst som det behövs.

Läs mer om inriktningen för de olika granskningsformerna i *Dataskyddsombudets inriktning och årshjul 2021-2022* (2021-06-29, dnr KS 2021/0313).

Syfte

Det övergripande syftet för granskningen är att stimulera till lärande och handlingsberedskap som stärker dataskyddet i verksamheten. Med utgångpunkt i granskningen ges råd och rekommendationer som dels kan bidra till att stärka redan fungerande delar i dataskyddet, och dels omhänderta avvikelser. Ett aktivt dataskyddsarbete som reflekteras och kontinuerligt stärkts innebär en stor trygghet för dem vars personuppgifter verksamheten hanterar.

Upplägg och metodik

Granskningen har främst gjorts genom en genomgång av dokumenterade rutiner, information och beskrivningar av dataskyddsarbetet inom nämndens ansvarsområde som förvaltningen ingett. Därutöver har jag själv även inhämtat uppgifter genom publicerad information på intranät och webbplats samt diarium. Dokumentationen som ingått i granskningen har varit sådan som visar på införlivandet av GDPR utifrån de områden som granskas. Exempel på dokumentation som ingått är delegationsförteckning, reglemente, dokumenthanteringsplan, personuppgiftsbiträdesavtal och dokumenterade arrangemang vid gemensamt personuppgiftsansvar, årshjul för dataskyddsarbetet, egenkontroller och ledningens genomgång, information till registrerade, utbildningsmaterial och vägledning till personal, rutinbeskrivning för hantering av personuppgiftsincidenter och handläggning av registrerades åberopade rättigheter.

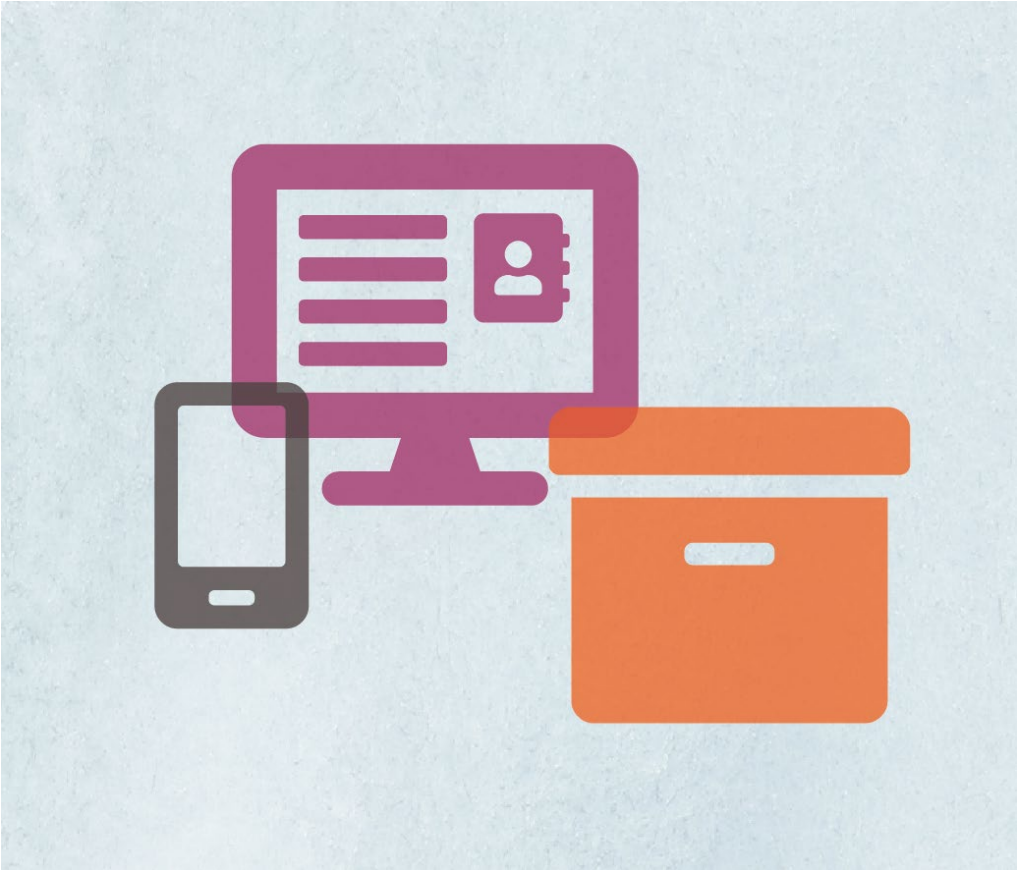
Därutöver har även en muntlig avstämning skett med verksamhetens dataskyddskontakt, förvaltningschef och avdelningschef utifrån de områden som ingått i granskningen. Metodiken för granskningen har byggt på en behovsbaserad arbetsgång som innebär att vidare utredning skett inom de områden där det under granskningen framkommit indikation på avvikelse.

[3] Mindre omfattande verksamheter är undantagna i 2021 års regelbundna granskning till fördel för andra insatser inom ramen för dataskyddsombudets råd och stöd.

Granskningen har genomförts under oktober-november 2021. I nästkommande granskning hösten 2022 kan mer verksamhetsnära granskningsmetoder komma att användas för att bättre fånga hur dataskyddet fungerar i verksamhetens vardag.

RUTINER FÖR ATT FÖLJA DATASKYDDSFÖRORDNINGEN

Så handskas vi med personuppgifter inom FG



Innehåll

1 Inledning 5
1.1 Versioner 5

2 Dataskyddsförordningen är en integritetslagstiftning 6
2.1 Begrepp 7
2.1.1 Laglighet och öppenhet 7
2.1.2 Ändamålsbegränsning 8
2.1.3 Uppgiftsminimering 8
2.1.4 Lagringsminimering 8
2.1.5 Integritet och konfidentialitet 8
2.1.6 Korrekthet 9
2.1.7 Ansvarsskyldighet 9
2.2 Lär dig mer 9

3 Våra personuppgiftsbehandlingar 10
3.1 Dokumentation över Förskola & Grundskolas personuppgiftsbehandlingar 10
3.2 Är behandlingarna som du kommer i kontakt med godkända? 10
3.3 Så gör du om en behandling du gör inte finns med 11
3.4 Konsekvensbedömning 11

4 Personuppgifter i verksamheten 12
4.1 Våra lagliga grunder 12
4.1.1 Allmänt intresse 13
4.1.2 Rättslig förpliktelse 13
4.1.3 Myndighetsutövning 13
4.1.4 Avtal 13
4.1.5 Samtycke 13
4.2 Personuppgifter och personuppgifter 14
4.2.1 Känsliga personuppgifter 14
4.2.2 Särskilt skyddsvärda personuppgifter 15
4.2.3 Sekretessreglerad information 15
4.3 Foto, film och ljudupptagning 16
4.3.1 Minnesfotografier 18
4.3.2 Fotografering när media besöker verksamheten 19
4.3.3 Kamerabevakning 19
4.3.4 Mer information 21
4.4 Verksamhetssystem och tjänsteleverantörer 21
4.5 Rätten till information 21

5 Gallra, rensa och spara 23
5.1 Vägledning om att rensa bland sparade personuppgifter 23
5.2 Exempel på rensningsarbete när det gäller dokument med personuppgifter 23
5.2.1 Arbetsmaterial 23
5.2.2 Mejl med integritetskänsliga uppgifter 24
5.2.3 Skanning 24
5.3 Dokumenthanteringsplan 25

6 Digitaliseringen och dataskyddet 26
6.1 Digitaliseringen och persondata 26
6.2 Appar för lärande 27
6.3 Kontohantering för elever 27
6.4 Våra verksamhetssystem 28
6.4.1 IST – barn- och elevregister 28
6.4.2 Vklass – pedagogiskt kommunikations- och dokumentationssystem 28
6.4.3 PMO – elevhälsans dokumentationssystem 29

6.4.4 Ciceron – vårt diarie- och ärendehanteringssystem 29
6.4.5 Microsoft Office 365 – vårt kommunikations- och samarbetssystem 29

7 Incidentrapportering 33
7.1 Sänd anmälan till forskola.grundskola@kungsbacka.se 33
7.2 Utredning 33
7.3 Åtgärda 34
7.4 Anmäl delegationsbeslut till nämnd 35

8 Rutin vid begäran om registerutdrag, återkallande av samtycke m.m. 36

9 Tjänsteleverantörer 37

10 Kvalitetssäkring 38
10.1 Årshjul 38

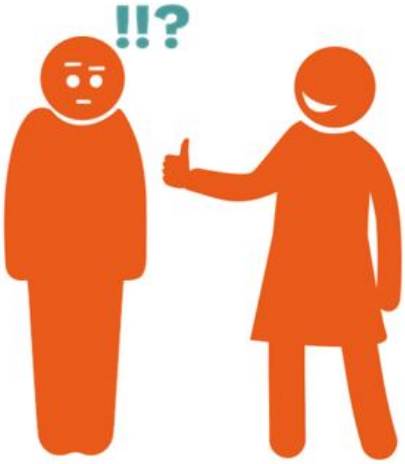
11 Organisering och ansvar 40
11.1 Personuppgiftsansvarig och dataskyddsombud 40
11.2 Dataskyddskontakt 40
11.3 Systemförvaltare/motsvarande 41
11.4 Registerbeskrivningsansvarig 41
11.5 Medarbetare 41
11.6 Chef 42
11.7 Förvaltningsledning 42

1 Inledning

Det här dokumentet beskriver samlat de rutiner och arbetssätt som vi har inom Förskola & Grundskola för att följa dataskyddsförordningen och värna våra barns, elevers, dess vårdnadshavares och anställdas integritet. Dokumentet uppdateras både vid behov och i halv- och helårsskifte.

1.1 Versioner

Datum	***Författare***	***Version***	***Ändringsbeskrivning***
190211	Karin Malmsten	1	Ny
190527	Karin Malmsten	1.1	Komplettering
191022	Karin Malmsten	1.2	Komplettering och korrektur
200617	Karin Malmsten	1.3	Komplettering och korrektur
201217	Karin Malmsten	1.4	Komplettering och korrektur



2 Dataskyddsförordningen är en integritetslagstiftning

Dataskyddsförordningen[1] är en EU-gemensam lag som gäller i Sverige som medlemsland från den 25 maj 2018. Den ersätter den tidigare gällande personuppgiftslagen (PuL) och kompletteras med dataskyddslagen[2].

Syftet med lagen är att skydda varje enskild EU-medborgares integritet och stärka individens rättigheter vid behandling av personuppgifter. Enligt artikel 8 i Europakonventionen har var och en rätt till respekt för sitt privatliv. Den snabba tekniska utvecklingen och omfattningen av behandling av personuppgifter ligger till grund för att ett regelverk som ska säkerställa en god skyddsnivå har kommit till.

Rätten till personlig integritet finns även med i FN:s konvention om de mänskliga rättigheterna och i Barnkonventionen. Detta speglas även i vårt uppdrag som utbildningsanordnare genom skollagens portalparagrafer och i läroplanen – både vad gäller de värden som vi genom utbildningen ska förankra hos våra barn och elever, och sättet på vilket vi ska genomföra den i våra olika verksamheter:

> *Utbildningen inom skolväsendet syftar till att barn och elever ska inhämta och utveckla kunskaper och värden. Den ska främja alla barns och elevers utveckling och lärande samt en livslång lust att lära. Utbildningen ska också förmedla och förankra respekt för de mänskliga rättigheterna och de grundläggande demokratiska värderingar som det svenska samhället vilar på. (1 kap. 4§ skollagen (2010:800))*
>
> *Utbildningen ska utformas i överensstämmelse med grundläggande demokratiska värderingar och de mänskliga rättigheterna som människolivets okränkbarhet, individens frihet och integritet, alla människors lika värde, jämställdhet samt solidaritet mellan människor.*
>
> *Var och en som verkar inom utbildningen ska främja de mänskliga rättigheterna […](1 kap. 5§ skollagen)*

Rätten till integritet är en grundförutsättning för demokrati. Inskränks denna rättighet genom till exempel avlyssning mot befolkningen hotas individernas personliga integritet och därmed även demokratin i samhället. Individens förmåga att undandra sig insyn från omgivningen, att ha kontroll över och tilltro till sina konfidentiella kommunikationer, är kopplad till både utvecklandet av självständiga ställningstaganden och fri åsiktsbildning.

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
[2] SFS 2018:218 Lag med kompletterande bestämmelser till EU:s dataskyddsförordning

Ett nytt, 26:e kapitel har alltsedan dataskyddsförordningens införande även införts i skollagen. Detta kapitel klargör i korta drag att det är tillåtligt att behandla de personuppgifter som krävs för att fullgöra uppdraget enligt skollag och läroplan och att den behandling som görs ska ske i enlighet med dataskyddsförordningen.

2.1 Begrepp

Begreppet *behandla personuppgifter* har en bred innebörd och innebär allt man gör men personuppgifter; samla in dem, registrera dem, lagra, bearbeta, sprida och radera dem.

Via denna länk hittar du en ordlista med de begrepp som används i dataskyddsförordningen - Ordlista

Dataskyddsförordningen bygger på ett antal grundläggande principer som ska genomsyra all vår personuppgiftsbehandling. Principerna ska vara vår ledstång när i vår verksamhet handskas med personuppgifter – oavsett om det rör barns/elevers uppgifter, vårdnadshavares, anställdas eller andras personuppgifter. Principerna är:

2.1.1 Laglighet och öppenhet

Denna princip handlar om att det måste finnas en **laglig grund** för behandlingen. Inom Förskola & Grundskola baserar vi vår behandling på de lagliga grunderna *rättslig förpliktelse*, *allmänt intresse*, *myndighetsutövning* och *avtal* (exempelvis anställningsavtal). Endast i mycket liten utsträckning är det aktuellt för oss att använda den lagliga grunden *samtycke* i vår verksamhet. Bara i samband med att barn eller elever medverkar på identifierbara bilder i syfte att informera om verksamheten i externa kanaler, eller i andra undantagssituationer, kan detta vara aktuellt.

Den registrerade måste få **information** om och **insyn** i vilka behandlingar som han eller hon förekommer i på ett tillgängligt och tydligt sätt.

Ta del av informationen på www.kungsbacka.se/Utbildning-och-barnomsorg/ Där ger vi information om hur vi behandlar personuppgifter inom Förskola & Grundskola.

2.1.2 Ändamålsbegränsning

Den här principen handlar om att ändamålen för behandlingen ska **vara klart i förhand**, vara **befogade** och **dokumenterade skriftligt** i en så kallad förteckning över personuppgiftsbehandlingar. Personuppgifterna får inte behandlas för andra syften än de ursprungligt avsedda.

Ta del av Förskola & Grundskolas förteckning via Insidan.

2.1.3 Uppgiftsminimering

Den här principen handlar om att personuppgifterna **inte får vara för omfattande** i förhållande till de ändamål som de behandlas för. Förskola & Grundskolas förteckning över personuppgiftsbehandlingar tydliggör vilka personuppgifter som får behandlas i de olika syftena – exempelvis olika identitetsuppgifter, kontaktuppgifter och känslig information.

2.1.4 Lagringsminimering

Den här principen handlar om att personuppgifterna får **inte sparas längre än vad som är nödvändigt**. När de inte längre behövs för ändamålet så ska de raderas. Det finns dock regler i arkivlagen och andra speciallagar (till exempel bokföringslagen) som innebär att personuppgifter som förekommer i vissa handlingar ska sparas viss tid eller bevaras för all framtid. Då är det den lagringstiden som är nödvändig.

Ta del av Förskola & Grundskolas dokumenthanteringsplan för hur länge olika handlingar ska sparas och var.

2.1.5 Integritet och konfidentialitet

Den här principen handlar om att personuppgifterna ska **skyddas** mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada.

Det innebär bland annat att **lämpliga tekniska och organisatoriska skyddsåtgärder ska finnas och användas**. Exempel sådana skyddsåtgärder är behörighetsstyrning och autentisering i system, kryptering, lösenordsskydd och anvisningar till personalen om hur man får handskas med uppgifterna.

Följ anvisningarna om i vilka system som olika personuppgifter får hanteras och behandlas och hur du som medarbetare ska spara dokumentation på ett säkert sätt och se till ingen obehörig kommer åt integritetskänsliga uppgifter via dina konton.

Du hittar anvisningarna i detta dokument men också i kommunens regler för Informationssäkerhet via Insidan

2.1.6 Korrekthet

Den här principen handlar om att vi ska noggranna med att personuppgifter som vi behandlar är rätta och riktiga, och vara snabba på att rätta dem om det framkommer att de är felaktiga.

2.1.7 Ansvarsskyldighet

Den här principen handlar om att vi inom Förskola & Grundskola inte bara ska följa dataskyddsförordningen utan även kunna **visa hur** vi följer den, att vi är ”compliant” och följsamma.

Ta för vana att i olika sammanhang ta upp dataskyddsfrågor vid arbetsmöten och liknande i din verksamhet för att hålla rutinerna runt personuppgiftsbehandlingen vid liv och främja integritetskulturen. På övergripande nivå görs även analyser och uppföljningar som ligger till grund för löpande risk- och förbättringsarbete.

2.2 Lär dig mer

På SKR och Datainspektionens hemsidor finns mer information. Varje personuppgiftsansvarig verksamhet måste dock själv göra en bedömning och ta ställning till vad som ska gälla i verksamheten. På FG:s dataskyddssidor på Insidan finns all dataskyddsrelaterad information samlad för medarbetare och där finns även ett material som kan användas på APT eller liknande.

3 Våra personuppgiftsbehandlingar

I detta avsnitt hittar du information om Förskola & Grundskolas förteckning över personuppgiftsbehandlingar och hur den ska vara ett stöd för dig att följa dataskyddsförordningens bestämmelser.

3.1 Dokumentation över Förskola & Grundskolas personuppgiftsbehandlingar

I förteckningen över personuppgiftsbehandlingar dokumenterar vi de personuppgifter som vi behandlar inom Förskola & Grundskola. Vi beskriver varför de behandlas, i vilka verksamhetssystem och med vilket lagstöd samt vilka kategorier av uppgifter och registrerade som omfattas. Vi dokumenterar även hur säkerheten runt uppgifterna är uppbyggt, vilka som använder dem och om uppgifterna överförs till andra myndigheter eller biträden samt om de i samband med detta överförs till länder utanför EU/EES (tredje land).

Syftet med dokumentationen är att vi inom Förskola & Grundskola ska ha kontroll över att de personuppgiftsbehandlingar som vi gör inom vår verksamhet är berättigade och följer de krav som finns. Förteckningen över behandlingarna uppdateras minst en gång varje termin och publiceras i samband med detta på Insidan och på Förskola & Grundskolas sidor på kungsbacka.se.

3.2 Är behandlingarna som du kommer i kontakt med godkända?

Bestämmelserna i dataskyddsförordningen innebär att det bara är de behandlingar som har dokumenterats i förteckningen som är godkända. I förteckningen är de olika behandlingarna upptagna utifrån att de uppfyller de säkerhetskrav som ställs

beroende på känsligheten och omfattningen i de uppgifter som förekommer i behandlingen.

Den absoluta merparten av de behandlingar som vi behöver göra inom Förskola & Grundskola är dokumenterade och säkerställda i förteckningen. Det kan dock förekomma behandlingar som inte kommit fram i arbetet med att kartlägga personuppgiftsbehandlingen i vår verksamhet, som tillkommit därefter, är mer tillfälliga eller som förändrats. Det kan också förekomma att behandlingar som tidigare gjorts inte har kunnat motiveras utifrån vårt uppdrag och att behandlingen av den anledningen inte längre är tillåtlig.

Som medarbetare måste du stämma av så att de personuppgiftsbehandlingar som du behöver göra i just ditt arbete finns upptagna i förteckningen.

3.3 Så gör du om en behandling du gör inte finns med

Om du inte hittar alla de behandlingar som du kommer i kontakt med i ditt arbete och som du anser är nödvändiga för dig att göra ska du anmäla det så att behandlingen kan kvalitetssäkras.

Vänd dig till:
Karin Malmsten, dataskyddskontakt karin.malmsten@kungsbacka.se

Beskriv vilka personuppgifter som behandlingen omfattar och vilka eventuella system som det gäller. Beskriv också varför du anser att behandlingen är nödvändig. Tillsammans reder vi ut om behandlingen redan finns med i förteckningen, om den behöver förtecknas, om behandlingen helt enkelt inte är tillåtlig därför att den till exempel faller utanför verksamhetens uppdrag eller att behandlingen inte faller inom dataskyddsförordningens tillämpningsområde.

3.4 Konsekvensbedömning

Inför ny personuppgiftsbehandling, eller i samband med förändrade förutsättningar kring befintlig behandling som inbegriper integritetskänslig information, ska en bedömning av risk och konsekvens göras, en så kallad DPIA.

I regel är det systemförvaltare eller motsvararande processansvarig som ansvarar för att en sådan analys görs. En dokumentmall med bedömningsstöd finns som bör användas. Det är också bra att ta del av Datainspektionens vägledning för vad en konsekvensbedömning ska innehålla.

Ta alltid kontakt med dataskyddskontakt för att få stöd när det är aktuellt att göra en konsekvensbedömning. Dataskyddskontakten hjälper till att bereda analysen inför inhämtandet av dataskyddsombudets bedömning som ska ingå. Kontakt behöver kanske också tas med IT eller andra som har kunskap runt förutsättningarna för behandlingen.

4 Personuppgifter i verksamheten

För att säkerställa att de barn och elever som finns i vår verksamhet får en utbildning och omsorg av hög kvalitet behöver vi som arbetar i verksamheten i flera olika sammanhang hantera både barns, elevers och deras vårdnadshavares personuppgifter.

I många av dessa behandlingar behövs även personuppgifter på dig som anställd. Exempelvis om du är betygssättande lärare så krävs det att det framgår av betygskvittensen att det är du som har satt betyget och ingen annan. Ditt namn, din roll och vilken enhet du arbetar vid kan också behövas om du är en aktör i att tillgodose en elevs behov av stöd, eller har tagit emot uppgifter om att ett barn eller elev upplever sig utsatt för kränkande behandling. Det krävs helt enkelt för att kunna fullgöra uppdraget som utbildningsanordnare och av dig som anställd för att vara en del i att uppfylla detta uppdrag.

För att få behandla personuppgifter krävs att den som är personuppgiftsansvarig har laglig grund att behandla uppgifterna. Vi behandlar alltså endast personuppgifter i den utsträckning det är nödvändigt för att fullgöra vårt uppdrag både som utbildningsanordnare och som arbetsgivare, samt för att uppfylla rätten till information om den behandling som görs.

4.1 Våra lagliga grunder

För de behandlingar av personuppgifter som sker inom Förskola & Grundskolas ansvarsområde gäller främst de lagliga grunderna *allmänt intresse*, *rättslig förpliktelse*, *myndighetsutövning* och *avtal*. Behandling som görs med stöd av dessa

grunder kan man som registrerad inte invända mot. Däremot kan man begära att få felaktiga uppgifter om sig korrigerade och rättade.

I enstaka situationer kan behandlingen basera sig på *samtycke*. I detta fall är behandlingen frivillig och den registrerade har rätt att återkalla sitt samtycke för att behandlingen ska upphöra.

Här finns information om vad de olika grunderna betyder.

4.1.1 Allmänt intresse

Att tillhandahålla, anordna och bedriva utbildning är i många fall en uppgift av **allmänt intresse**. Vad som är allmänt intresse utgår alltid från nationell rätt i någon form. Att kunna följa upp utbildningen för att utveckla och förbättra den motiverar till exempel att personuppgifter behandlas i till exempel enkäter, eller genom att information om satta betyg sammanställs. Dessa baserar sig då på den lagliga grunden *allmänt intresse* utifrån utbildningens syfte och barns och elevers rätt rent generellt till en likvärdig och god utbildning i trygg miljö.

4.1.2 Rättslig förpliktelse

I många fall är det nödvändigt för oss att behandla personuppgifter för att kunna fullgöra utbildningen enligt de mer specifika krav som ställs på utbildningen utifrån skollagen eller andra speciallagar, exempelvis för att utreda behov särskilt stöd. I dessa fall baseras behandlingen på den lagliga grunden **rättslig förpliktelse**.

4.1.3 Myndighetsutövning

I vår verksamhet vidtar vi också vissa åtgärder med stöd av skollagen som innebär myndighetsutövning, till exempel betygssättning, beslut om särskilt stöd och beslut om disciplinära åtgärder. Den behandling av personuppgifter som är nödvändig för myndighetsutövningen görs i dessa fall med stöd av den lagliga grunden **myndighetsutövning**.

4.1.4 Avtal

När det gäller de personuppgifter som rör dig som anställd baseras de i huvudsak på **avtal** utifrån att du i ett anställningsavtalsförhållande förväntas utföra de arbetsuppgifter som hör till tjänsten.

4.1.5 Samtycke

Den lagliga grunden **samtycke** används i vår verksamhet i mycket begränsad utsträckning. Behandlingar som görs baserat på att elever och vårdnadshavare samtyckt till behandlingen kan förekomma när skolan tar identifierbara foton för att

lägga ut på sin hemsida, helt enkelt i situationer där behandlingen av uppgifterna inte är knuten till en uppgift att fullgöra utbildningen enligt de krav som ställs i författning eller förordning.

Ett samtycke ska alltid vara aktivt, frivilligt, specifikt och informerat (en otvetydig viljeyttring) och det ska när som helst kunna återkallas. Om det görs, alltså återkallas, ska vi inte längre att behandla personuppgifterna i det syfte som tidigare gjorts med stöd i samtycket. Kravet på skydd är lika stort vid samtycke som vid en behandling som baseras på en annan laglig grund och man kan därför inte samtycka till en lägre skyddsnivå i hanteringen.

Utgångspunkten är att vi inte ska behandla personuppgifter med stöd av samtycke annat än när det i undantagsfall bedöms befogat. Band annat eftersom barn, elever och vårdnadshavare i vår verksamhet står i beroendeställning till oss och vårt uppdrag är så pass lagbundet.

4.2 Personuppgifter och personuppgifter

Många uppgifter räknas som personuppgifter. Alla uppgifter som direkt eller indirekt kan identifiera en fysisk person räknas och det kan röra sig om allt från rena identitetsuppgifter såsom namn eller personnummer, kontaktuppgifter såsom hemadress eller telefonnummer till värderande information såsom hälsotillstånd eller bedömningar om prestationer.

Vissa uppgifter är mer integritetskänsliga än andra och dessa kan grovt delas in i tre kategorier; *känsliga personuppgifter* enligt dataskyddsförordningen, *särskilt skyddsvärda personuppgifter* och *sekretessreglerade uppgifter.* Sådana uppgifter måste vi vara särskilt aktsamma om och hantera endast med förstärkta tekniska och organisatoriska skyddsåtgärder. Ingen annan än de personer som behöver uppgifterna i sitt arbete ska ha tillgång till dem, och de får inte delas eller spridas utanför avsett verksamhetssystem utan skydd i form av exempelvis kryptering.

Det är inte bara dataskyddsförordningen vi ska ta hänsyn till när det gäller integritetskänslig information om elever, vårdnadshavare och anställda i vår verksamhet. Offentlighets- och sekretesslagstiftningen ska tillämpas samtidigt med dataskyddsförordningen.

4.2.1 Känsliga personuppgifter

Känsliga uppgifter enligt dataskyddsförordningen utgörs av uppgifter om ras/etniskt ursprung[3], politiska åsikter, religiös/filosofisk övertygelse, medlemskap i fackförening, hälsoinformation, sexualliv, brott/brottsmisstanke, genetiska uppgifter, biometriska uppgifter.

[3] I svenska lagar använder vi inte längre ordet ras. I dataskyddsförordningen används ordet, men det står också att det inte innebär att EU godtar teorier om att det skulle finnas skilda människoraser.

4.2.2 Särskilt skyddsvärda personuppgifter

Särskilt skyddsvärda uppgifter är sådana uppgifter som visserligen inte är känsliga i dataskyddsförordningens mening ovan, men som behöver skyddas med bättre säkerhetsåtgärder än mer harmlös information. Exempel på extra skyddsvärd information är integritetskänsliga uppgifter såsom omdömen och värderande information om exempelvis prestationer och förmågor, personlighetsprofiler, personnummer, viss ekonomisk information eller annan information som ligger nära privatlivet.

I vår verksamhet utgör exempelvis *underlag* för kunskapsbedömning såsom provresultat eller kommunikation omkring skolarbetet ingen känslig eller extra skyddsvärd information. Däremot kan den *bedömning* av elevers kunskaper och färdigheter som görs betraktas som extra skyddsvärd och integritetskänslig information.

Personuppgifter om barn – oavsett om det handlar om harmlösa eller skyddsvärda uppgifter – är samtidigt alltid att betrakta som extra skyddsvärda. Detta eftersom barn befinner sig i särskild beroendeställning och inte alltid själva kan tillvarata sina rättigheter. Ju yngre barnet är desto mer skyddsvärda är uppgifterna, och vi ska därför rent generellt vara varsamma med barns och elevers personuppgifter över huvud taget, även om det inte alltid behöver innebära att integriteten kränks om personuppgifter röjs på ett sätt som inte varit avsett.

4.2.3 Sekretessreglerad information

Dessutom omfattas vissa uppgifter av **sekretess** av olika grad, och för vår verksamhet gäller offentlighets- och sekretesslagen (OSL). Denna lagstiftning tar i första hand sikte på karaktären av olika information och ska tillämpas *tillsammans med* dataskyddsförordningen, som i sin tur framför allt tar sikte på personuppgifter som behandlas elektroniskt.

Inom förskolan omfattas till exempel *all* dokumentation om barnen och vårdnadshavarna av stark sekretess, medan det inom grundskolan generellt gäller en svagare sekretess. Den elevstödjande verksamheten inom grundskolan omfattas dock av stark sekretess, och inom elevhälsans medicinska område omfattas informationen av absolut sekretess vilket innebär är en ännu starkare sekretessgrad.

• **Absolut sekretess** betyder att *inga uppgifter* under *några förutsättningar* får lämnas ut till andra än de anställda som behöver uppgifterna för att kunna utföra sitt arbete. Utlämnande kan dock ske till den enskilde själv eller vårdnadshavare efter sekretessprövning.

• **Stark sekretess** betyder att *uppgifterna i första hand omfattas av sekretesskydd* och att uppgiften endast får lämnas ut om det står klart att det kan ske *utan att visst men eller viss skada uppkommer*.

• **Svag sekretess** betyder att det är *offentlighet som gäller i första hand* och att uppgiften endast får sekretessbeläggas om det kan antas att visst men eller viss skada kan uppstå.

4.3 Foto, film och ljudupptagning

Foto, film och även ljudupptagning där fysiska personer kan identifieras utgör personuppgifter. Därför gäller dataskyddsförordningen även när vi använder dessa medier. Några grupper i samhället är särskild skyddsvärda när det gäller hantering av personuppgifter. Barn är en sådan grupp. Det betyder att vi generellt sett alltid ska vara särskilt varsamma med dessa uppgifter. Då personuppgifter i form av foto, film och ljudupptagning kan bilda underlag till insamling av biometriska uppgifter (för exempelvis ansikts- och röstigenkänning) ska vi också vara särskilt varsamma med spridningen av sådana uppgifter och endast behandla uppgifterna i interna, slutna system.

Behandling av personuppgifter i form av foto inom vår verksamhet får endast förekomma i följande situationer:

1. När det är nödvändigt för att dokumentera och bedöma barns/elevers kunskapsutveckling

Denna behandling baseras då på de lagliga grunderna *Rättslig förpliktelse* (dokumentationen) samt *Myndighetsutövning* (bedömningen) och är inget som en elev eller vårdnadshavare samtycker till. Självfallet ska vi dock ta hänsyn till barn/elever som har identitetsskydd eller som av en annan anledning känner obehag inför att medverka på foto/film/ljudupptagning.

I förteckningen av personuppgiftsbehandlingar ingår detta under ändamålet *Bedöma och dokumentera barns och elevers kunskapsutveckling*.

Precis som med övrig dokumentation av ett barns eller en elevs kunskapsutveckling ska materialet då inte vara tillgängligt för andra elever och dess vårdnadshavare.

2. När det behövs för att åskådliggöra vad en grupp åstadkommit och lärt tillsammans. Detta görs utifrån *Rättslig förpliktelse* och i förteckningen över behandlingar ingår detta under ändamålet *Möjliggöra elevers och lärares kommunikation om undervisningen.*

Foton som publiceras elektroniskt på en gemensam yta får endast visa lärandet och det som görs utan att enskilda individer är identifierbara.

Film- och ljudupptagningar som behövs i detta syfte, där många barn/elever medverkar, är svårare att avidentifiera och ska därmed inte publiceras elektroniskt alls. Däremot kan det användas i verksamheten via lärplatta och

dator. Det kan också återges för vårdnadshavare i samband med exempelvis föräldramöten, drop-in i verksamheten eller vid utvecklingssamtal.

3. När det behövs för att identifiera barn och elever i verksamheten för att exempelvis vikarier eller personal som inte dagligen möter eleverna i verksamheten ska kunna möta upp dem på ett bra och betryggande sätt (exempelvis personal inom elevhälsan). Det kan också utgöra ett stöd i skolans trygghetsarbete i övrigt.

Denna behandling baseras också på *Rättslig förpliktelse* och *Allmänt intresse* och återges i förteckningen över behandlingar som *Identifiera barn och elever i verksamheten*.

Fotografering som görs i detta syfte kan antingen genomföras genom att skolans personal själva fotograferar barnen/eleverna och sedan lägger in bilderna i elevregistersystemet IST. Om fotografierna behöver mellanlagras någonstans kan det göras på skolans Sharepoint-sida. Därefter ska fotona raderas därifrån.

När fotografierna är inlagda i IST kan en klasslista med fotografier sedan genereras, som kan skrivas ut för vikarier och personal som inte har åtkomst i systemet.

Fram till dess att funktionaliteten för detta är klart i IST läggs bilderna på skolans Sharepoint-sida, där de också kan monteras i en förmallad fotokarta. Mallen finns tillgänglig via Förskola & Grundskolas dataskyddsidor på Insidan.

Foton som tas i detta ändamål behöver inte tas om varje år, utan fotografierna används så länge de är användbara i syftet att identifiera barnen/eleverna. När fotona inte längre är användbara eller behövs för ändamålet ska de ersättas eller raderas (se Förskola & Grundskolas dokumenthanteringsplan). Exempelvis när barnet/eleven blivit äldre eller slutar i verksamheten.

Inget hindrar att skolan för själva fotograferingen anlitar en fotograf, antingen kommunfotografen eller fotograf utanför kommunens organisation. Uppdraget ska då också omfatta att leverera fotografierna i ett läsbart format och innebära att fotografen direkt efter bekräftad leverans raderar fotografierna.

Om skolan uppdrar till kommunfotografen ska Förskola & Grundskolas kommunikationsavdelning kontaktas för att göra beställningen, och om en fotograf utanför kommunens organisation anlitas ska dataskyddskontakt kontaktas för att upprätta ett pub-avtal. Kostnaden för att anlita fotograf ansvarar förskolechef/rektor för.

4. I undantagsfall fall kan vi fotografera elever för att publicera på till exempel hemsidan och för detta tillfälle ta in ett samtycke från vårdnadshavarna. En bedömning ska då göras i varje enskilt fall om det kommunikativa värdet är tillräckligt starkt. Exempel på detta skulle kunna vara att publicera foto och

namn på elever som vunnit en renommerad tävling eller deltagit i ett projekt som anses vara av stort intresse för allmänheten.

I övrigt har vi som utgångspunkt att inte behandla personuppgifter i form av foto, film och ljudupptagning på barn och elever i vår verksamhet. Att sprida foto och film på hemsida eller socialt media är inte nödvändigt för att uppfylla syftet och målen för utbildningen. Av samma anledning ska inte heller fotografering ske där ett fotoföretag erbjuder fotografierna som skolan behöver till vidare försäljning. Skolfotografering av detta slag har vi utrett särskilt inom Förskola & Grundskola och bedömt som en behandling som av många skäl inte kan betraktas som berättigad. Dels utifrån dataskyddsförordningens krav, men också utifrån andra aspekter såsom likvärdig tillgång till utbildning.

4.3.1 Minnesfotografier

Många elever och föräldrar vill gärna ha minne från skoltiden i form av porträtt- och/eller gruppfotografier. Föräldraföreningar som vill arrangera porträtt- eller gruppfotografering i samband med till exempel en sommaravslutning kan göra det och skolan kan upplåta lokal för det. Det är också föräldraföreningen som i sådana fall anlitar fotograf. Beroende på situation kan antingen föräldraföreningen eller fotografen vara personuppgiftsansvarig. Fotografen eller föräldraföreningen kan be att få ut klass/grupplistor från skolan, vilket lämnas ut enligt rutin med sedvanlig sekretessprövning.

Det är viktigt att fotograferingen inte görs som en del av skolans verksamhet och att det görs på ett sätt så att det är tydligt för var och en att fotograferingen är ett helt frivilligt inslag som arrangeras av föräldraföreningen och inte av skolan. Skolan/förskolan ska inte använda sig av de fotografier som tas eftersom det inte är skolan som anordnar fotograferingen.

Vid en fotografering som anordnas av en föräldraförening i samband med skolans lokaler/verksamhet måste skolan försäkra sig om att det finns möjlighet för de barn/elever som inte vill medverka att avstå på ett naturligt sätt. Skolan måste också försäkra sig om att fotograferingen inte äventyrar situationen för de barn/elever som har någon form av identitetsskydd. Fotografering som ordnas av föräldraförening ska till exempel inte ligga mitt i ett program/schema som skolan har gjort upp, utan ske efter skol/verksamhetstid.

Det finns inget hinder för en förskola/skola att i samband med avslutningar eller luciafirande ordna med en avskild fotograferingshörna där föräldrar själva kan fotografera sina egna barn och ge tillåtelse till att barnen även är med på foto tillsammans med andra barn.

Det är alltid förskolechef/rektor som beslutar om hur förskolas/skolans lokaler får användas och kan också besluta att ingen fotografering får äga rum alls. Finns personer i eller i verksamhetens närhet som har någon form av identitetsskydd gäller

alltid att iaktta försiktighet med fotografering, men förskolechef eller rektor kan även ha andra skäl till att besluta att fotografering inte får ske.

4.3.2 Fotografering när media besöker verksamheten

Intervjuer och fotografering som görs av grundlagsskyddade medier omfattas inte på samma sätt som Förskola & Grundskola av reglerna i förordningen. Det är medieföretaget som i dessa fall är personuppgiftsansvarig och inte Förskola & Grundskola. Vårdnadshavarna ska dock alltid informeras om pressens närvaro på skolan och tillfrågas vid varje enskilt tillfälle om barnet/eleven får vara med i intervju och/eller bild.

4.3.3 Kamerabevakning

Kamerabevakning i skollokalerna är en personuppgiftsbehandling som under vissa villkor är tillåtlig inom Förskola & Grundskolas grundskolor. Förutsättningen är att det sker som ett led i att komplettera skolans ordinarie trygghetsarbete när det inte finns andra sätt att få bukt med ordningen och studieron på skolan.

Kamerabevakning får aldrig ersätta eller utgöra grundstommen i skolans trygghetsarbete. Den får heller inte inledas eller fortgå utan att det finns ett reellt behov som inte kan tillgodoses på annat sätt. Det kan till exempel handla om omfattande skadegörelse eller intrång i lokalerna av obehöriga.

Rektor initierar frågan

Det är rektorn som väcker frågan om kamerabevakning som komplement i trygghetsarbetet och som redogör för de reella behov som finns på skolan.

Behoven föredras för Förskola & Grundskolas processansvarig för lokaler som med stöd av förvaltningens dataskyddskontakt bedömer om behoven är tillräckliga. Bedömningen dokumenteras i diarie- och ärendehanteringssystemet Ciceron och tillsammans går man igenom förutsättningarna kring installation, rutiner och finansiering.

Generellt om förutsättningarna runt kamerabevakning inom Förskola & Grundskola

Personuppgiftsbehandlingen som sker i samband med kamerabevakningen omfattar identifierande uppgifter i form av identifierbara filmbilder på elever och personal som vistas i de utbildningslokaler som är avsedda för skolpersonal och elever. Bevakningen omfattar alltså inte lokaler och utrymmen dit allmänheten har tillträde såsom expedition, rektorskontor och samordnat bibliotek. Kamerabevakningen omfattar inte heller integritetsutrymmen såsom toaletter och omklädningsrum.

Endast behörig personal kan ta del av filmmaterialet

Om kamerabevakning installeras på en skola är det endast utsedd behörig personal på skolan som kan begära att filmsekvenser tas ut och granskas i syfte att utgöra verifikat av utpekade händelser. Behörig är rektor och skolchef och/eller den som

rektor/skolchef delegerat uppgiften till. Uttag av filmmaterial kan alltså endast begäras på förekommen anledning och av personal som är behörig vidta åtgärder för att säkerställa trygghet och studiero.

Bevakningskamerorna ingår i en skyddad miljö och materialet som inte används raderas löpande

Varje enskild kamera som ingår i behandlingen installeras och driftas av kommunens IT- och servicecenter. Kamerorna ingår i ett fristående kameranätverk och filmmaterialet lagras på en egen, separat server. Filmmaterialet sparas endast under den period som det behövs för att främja trygghet och förebygga skadegörelse på skolan och maximalt 30 dagar. Därefter raderas informationen. Information som ingår i ett ärende, till exempel ordningsärende, diarieförs i det ärende den ingår och sparas beroende på vad det handlar om för typ av ärende[4].

Vid uttag av filmsekvenser som bildar underlag till ärende görs identifieringen av de personer som förekommer i materialet direkt. Utifrån detta avidentifieras personer som förekommer i filmmaterialet och som kan konstateras inte har med ärendet att göra eller har någon form av identitetsskydd. Detta görs av systemansvarig i samverkan med rektor och/eller skolchef.

Identifierbara personer i filmsekvensen som tillför ärendet, antingen genom att de visat sig ha en aktiv roll i exempelvis skadegörelse eller hot eller bevittnat händelsen, namnges i samband med registreringen av materialet i ärendehanteringssystemet. Det görs för att materialet ska bli sökbart i samband med exempelvis begäran av registerutdrag. Beroende på vad det handlar om för ärende anges aktuell sekretessgrund.

Filmsekvenser som inte visar information som leder till att ärende inleds raderas.

Elever, dess vårdnadshavare och personal på skolan informeras

Information om behandlingen till registrerade ges bland annat via Förskola & Grundskolas generella information om personuppgiftsbehandlingen på Kungsbackas offentliga webbplats. Information ges också specifikt till de registrerade som deltar i den verksamhet där behandlingen sker, exempelvis vid föräldramöten, klassinformation och personalmöten. Det sätts också upp väl synliga skyltar med information om att kamerabevakning sker i lokalerna, vem man kan kontakta om man har frågor samt hur man kommer i kontakt med dataskyddsombudet.

---

[4] Filmer som myndigheter skapar och färdigställer utgör på samma sätt som pappershandlingar allmänna handlingar. Samma regler blir därför tillämpliga även för filmer som skapas och färdigställs. Filmer som tillhör ett ärende blir allmänna när ärendet har slutbehandlats. Filmsekvenser som tas ut som verifikat av exempelvis skadegörelse ska därmed diarieföras i det ärende den tillhör. I övrigt ska inte uppgifter som upptas i löpande bevakningsfilm diarieföras eftersom materialet inte utgör ett färdigställt material.

Behandlingen omprövas regelbundet
Att behandlingen ska vara behovsbaserad innebär att behovet följs upp och aktualiseras årligen. För detta ansvarar Förskola & Grundskolas lokalutvecklingsansvarig. Behovsbedömningen dokumenteras i systemobjektet på samma sätt som den initiala behovsanalysen.

4.3.4 Mer information

För frågor om personuppgifter i form av foto, film och ljudupptagning kontakta förvaltningens kommunikatör eller dataskyddskontakt.

För frågor runt kamerabevakning inom Förskola & Grundskolas verksamhet kontakta utvecklingsledare inom lokalplanering eller dataskyddskontakt.

4.4 Verksamhetssystem och tjänsteleverantörer

För att uppfylla ändamålen med vår personuppgiftsbehandling delar vi ibland uppgifter med tjänsteleverantörer som tillhandahåller tjänster till Förskola & Grundskola, exempelvis i samband med systemdrift och systemsupport. Tjänsteleverantörerna får endast behandla personuppgifterna enligt våra instruktioner och inte använda uppgifterna för egna ändamål. De är även skyldiga enligt lag och avtal att i sin tur skydda uppgifterna. Med varje tjänsteleverantör avtalas detta i ett så kallat personuppgiftsbiträdesavtal (Pub-avtal).

4.5 Rätten till information

Inom Förskola & Grundskola följer vi regelbundet upp vår personuppgiftshantering och de dokumenterade behandlingarna justeras och rättas vid behov. Som registrerad har man bland annat rätt att få information om i vilka ändamål som personuppgifter knutna till sig behandlas, utifrån vilken grund och hur länge uppgifterna sparas.

Handlingar som innehåller personuppgifter sparas endast så länge det är nödvändigt, baserat på de arkivregler som omfattar offentliga handlingar och regler i andra författningar såsom exempelvis bokföringslagen. I Förskola & Grundskolas dokumenthanteringsplan finns information om hur länge och på vilket sätt som vi ska spara olika slags handlingar.

Genom att begära registerutdrag kan den registrerade själv ta del av vilka personuppgifter som behandlas och i vilka ändamål. Registerutdraget består av en översikt över de behandlingar som man förekommer i, samt det underlag som i sin helhet förekommer inom varje behandling. Arbetsmaterial och arkiverat material lämnas dock inte med i underlaget, och vid många liknande handlingar lämnas senast tillgängliga utdrag. Utdrag omfattande arkiverade uppgifter tillhandahålls av arkivet som egn myndighet/personuppgiftsansvarig.

Syftet med rätten att få registerutdrag är att den registrerade ska kunna få verifikat på att personuppgifterna om henne eller honom inte behandlas på annat sätt än vad som uppgett och att uppgifterna som behandlas är korrekta. Om uppgifterna är felaktiga ska den registrerade kunna begära att uppgifterna rättas eller raderas.

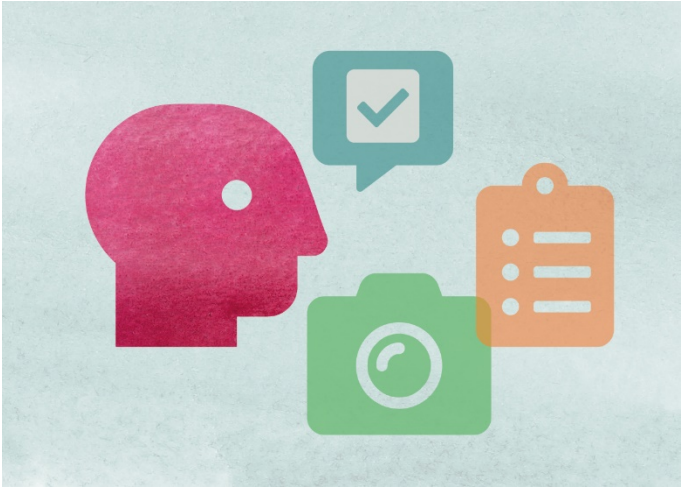
Som registrerad finns fler rättigheter och alla dessa tjänster kan man som registrerad beställa på Kungsbacka kommuns hemsida. Förfaringssättet är likadant oavsett vilken personuppgiftsansvarig nämnd det rör.

Kungsbacka kommuns dataskyddsombud

Som registrerad kan man alltid vända sig till Förskola & Grundskola om man har frågor kring dataskydd och hanteringen av personuppgifter inom verksamheten. Man kan också kontakta Kungsbacka kommuns dataskyddsombud.

Dataskyddsombudets uppgift är att granska att vi inom vår verksamhet följer de rutiner vi har och att rutinerna är förenliga med förordningen. Om man som registrerad har klagomål på hur vi inom Förskola & Grundskola hanterar personuppgifter är dataskyddsombudet därför en bra person att kontakta. Ytterst är det dock Datainspektionen som har tillsyn över hanteringen, och som registrerad har man även rätt att inge klagomål dit.

Kontakta dataskyddsombud på dataskyddsombud@kungsbacka.se



5 Gallra, rensa och spara

5.1 Vägledning om att rensa bland sparade personuppgifter

En viktig uppgift som var och en av oss har i vårt arbete är att löpande tänka på att rensa vår dator och OneDrive från olika sammanställningar som inbegriper personuppgifter som man hämtat ur system eller själv sammanställt för att kunna genomföra en arbetsuppgift. Detsamma gäller även personuppgifter som kommit till oss via e-post.

Två olika dokument beskriver var handlingar med personuppgifter hör hemma och hur de ska förvaras beroende på innehåll och karaktär. När du rensar din dator, OneDrive och e-post och är osäker på var och om den ska sparas är *förteckningen över behandlingar* och *dokumenthanteringsplanen* vägledande. Dessa dokument revideras löpande och finns på Insidan. Dokumenthanteringsplan

5.2 Exempel på rensningsarbete när det gäller dokument med personuppgifter

5.2.1 Arbetsmaterial

- Lärare som ur ett system drar ut en klasslista för att till exempel sammanställa bedömningsunderlag i form av provresultat ska inte mer än så länge det är nödvändigt för att kunna motivera en bedömning eller ett satt betyg, spara listan på sin OneDrive. Därefter ska listan slängas.
- Kartläggnings- och utredningsmaterial i olika elevärenden innehåller ofta personuppgifter och dessutom information av känslig karaktär. Detta material får inte finnas i hemkatalogen på datorn utan ska föras in i de system vi använder, exempelvis PMO, Vklass eller Ciceron.

  Viss sådan information som utgör arbetsmaterial kan dock tillfälligt förvaras i den egna ytan i OneDrive. Förutsättningen är att informationen krypteras.

  För att kryptera dokument och information är det viktigt att du följer de anvisningar som ges. Dessa anvisningar finner du via länken Förskola & Grundskola Kryptering
- Närvarolistor vid olika evenemang är ett annat exempel. Sådana listor behövs som underlag när vi redovisar inköp till evenemanget eller för att pricka av närvaro. Så snart evenemanget är avklarat och vi bifogat underlaget till en faktura ska listan raderas.

5.2.2 Mejl med integritetskänsliga uppgifter

Utgångspunkten i vår verksamhet inom FG är att vi ska vara mycket varsamma med att överföra uppgifter som innehåller extra skyddsvärd, känslig eller sekretessreglerad information via mejl.

Om det är nödvändigt att överföra information av känslig karaktär via e-post ska du som medarbetare vidta skyddsåtgärder kring den känsliga informationen genom att i första hand kryptera informationen i mejlen. För att kryptera dokument och information är det viktigt att du följer de anvisningar som finns. Dessa anvisningar finner du via länken

Förskola & Grundskola Kryptering

Information kan i undantagsfall mejlas till namngiven e-postadress hos myndighet inom eller utanför kommunens organisation.

Kom ihåg att alltid ta bort information som överförts via mejl från din egen utkorg.

Observera att integritetskänslig information till eller från skolsköterska eller psykolog inte ska mejlas alls, såvida inte en myndighet som det råder uppgiftsskyldighet till har begärt att få information så. Detta eftersom sekretessen inom dessa områden är särskilt sträng.

Mejla heller aldrig integritetskänslig information till privatpersoner, exempelvis om elever till vårdnadshavare. Ta istället en telefonkontakt eller boka ett möte om det är nödvändigt att diskutera integritetskänslig information.

Inkommande mejl som innehåller information av känslig karaktär eller som är sekretessreglerad får inte sparas i mejlen. Om det är uppgifter som behöver sparas ska de föras till det system och ärende informationen de hör hemma i, till exempelv PMO. Mejl som behöver diarieföras ska läggas in i diariet (systemet Ciceron). Mejlkorrespondens som lärare/mentor behöver spara under en period kan sparas på OneDrive med kryptering.

När du svarar på ett mejl med känsliga, särskilt skyddsvärda eller sekretessklassade uppgifter, till exempel personnummer, hälsoinformation eller liknande ska du alltid ta bort ursprungsmeddelandet i ditt svarsmejl, alternativt svara i ett nytt mejl att du mottagit informationen. Detta för att undvika att ytterligare sprida informationen.

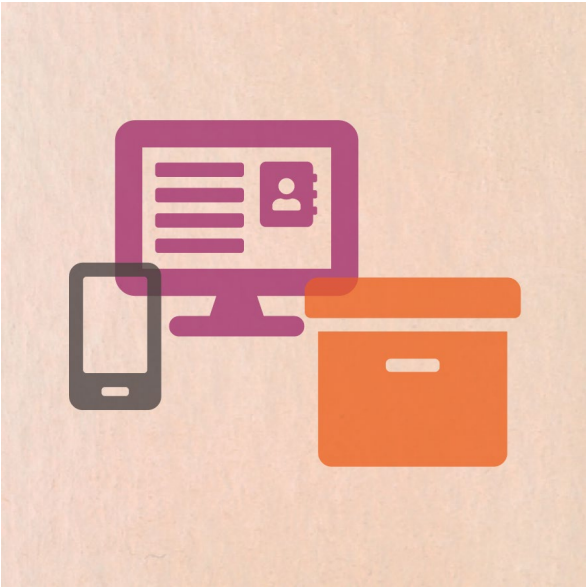
5.2.3 Skanning

Det är okej att skanna dokument innehållandes information av känslig karaktär från en skanner i det interna nätverket till mejlen. De inskannade filerna ska dock direkt omhändertas i rätt verksamhetssystem och därefter raderas från inkorgen och den eventuella mellanlagringsytan. Ta för vana att alltid tömma papperskorgen på datorn när du raderar dokumentfiler.

5.3 Dokumenthanteringsplan

Tillsammans med delegeringsförteckningen är dokumenthanteringsplanen styrdokument som behövs för att skapa struktur samt ordning och reda på våra dokument och beslut. Den är en förteckning över förvaltningens handlingstyper och ger instruktioner till medarbetare om hur information i form av dokument av olika slag och beslut i verksamheten ska hanteras; var och hur länge den ska bevaras.

Dokumenthanteringsplanen finns på Insidan Dokumenthanteringsplan



6 Digitaliseringen och dataskyddet

6.1 Digitaliseringen och persondata

I regeringens digitaliseringsstrategi och i den nya läroplanen för både förskola, fritidshem och grundskola har användning av och kunskap om modern informationsteknik och digitala verktyg lyfts fram som viktiga samhällskompetenser och därmed förstärkts. Tillgången till moderna kommunikations- och informationsverktyg betonas också i skollagen. Den nya förvaltningslagen innebär också att handläggningen av ärenden alltmer måste anpassa sig till digitala lösningar och i Regeringens strategi för en stark demokrati *Främja, Förankra, Försvara*, s 46 står bland annat följande:

”Vissa förmågor har blivit särskilt viktiga i digitala miljöer. Var och en måste ha kunskap om hur digitaliseringen påverkar oss. Alla behöver förstå och kunna utöva källkritik. Kunskap krävs om hur man skapar, använder och kommunicerar digitalt innehåll. En bättre teknikförståelse krävs, t.ex. om hur algoritmer fungerar. För en trygg digital miljö behöver alla ha kännedom om den lagstiftning som reglerar fri- och rättigheter och som skyddar den personliga integriteten.

[...]

Viktiga aktörer […] är **skolväsendet**, biblioteken, universitet och högskolor, medieföretagen, civilsamhället och folkbildningen, **kommuner** och landsting, liksom ett antal myndigheter och stiftelser.”

De många välfärdsutmaningar som framtiden bär med sig innebär att utvecklandet av samhällstjänster måste dra nytta av ny teknik och digitaliseringens möjligheter. I

detta sammanhang blir en respektfull hantering av personuppgifter och den personliga integriteten en avgörande förutsättning.

Inom Förskola & Grundskola pågår digitaliseringsinitiativ både för att anpassa och förbättra vår verksamhet genom digitala lär- och kommunikationsverktyg och för att förbereda barn och elever för ett alltmer digitaliserat. Det pågår också initiativ för att digitalisera servicen. Dataskyddsförordningen påverkar oss i arbetet genom att vi ska vara noggranna med att se över och gå igenom säkerheten vad gäller personuppgifter i de digitala verktygen och tjänsterna innan de används.

6.2 Appar för lärande

Applikationer (appar) och andra digitala lärverktyg som är genomlysta och godkända utifrån dataskyddsförordningens bestämmelser kan hämtas ur företagsportalen. Via länken nedan finns en sammanställning över appar och digitala lärverktyg och tjänster som godkänts (och vilka som inte gjort det) samt vilka som står på ”väntelistan” för att godkännas.

Lista godkända appar - finns i Sharepoint och uppdateras löpande

Medarbetare som upptäcker en app eller digitalt lärverktyg som man vill använda kan genom ett formulär anmäla detta. Anmälan görs till förvaltningens digitaliseringsenhet (pedagoger anmäler via IKT-pedagog) genom att man fyller i ett formulär för att utvärdera om appen eller verktyget går att använda ur dataskyddsförordningsperspektiv.

Länk till formulär/checklista

6.3 Kontohantering för elever

Elever har tillgång till lärverktyg och personligt konto med lagringsyta och kontaktmöjligheter i kommunens domän. Utifrån ett aktivt arbete i utbildningsverksamheten med att träna elever i hur de ska handskas med digitala verktyg och hur de ska hantera sina kontouppgifter och bete sig i det digitala rummet har årskurs 5 bedömts som en hållpunkt för när elever bör börja få eget ansvar för sina inloggningsuppgifter. Läs vidare i de rutiner som finns omkring kontohantering och digitala lärverktyg i kommunens grundskolor eller vänd dig till enheten för digitalt lärandestöd.

6.4 Våra verksamhetssystem

Huvuddelen av den hantering av personuppgifter som vi behöver göra inom vår verksamhet i Förskola & Grundskola täcks av våra verksamhetssystem. Det är här som de uppgifter och tillhörande dokumentation som i olika avseenden behövs för att fullgöra vårt uppdrag också ska göras. Nedan framgår vilka systemen är och vad de ska användas till.

För varje system finns systemförvaltare eller motsvarande vars uppgift är att underhålla och bevaka systemets funktionsduglighet och informationssäkerhet och ha löpande kontakt med leverantören. Inom Förskola & Grundskola följer vi Kungsbacka kommuns systemförvaltarmodell som bland annat innebär att systemförvaltarna ansvarar för att det finns rutiner för behörighetstilldelning, utbildning för användare, tillhandahålla registerutdrag, utreda och åtgärda eventuella personuppgiftsincidenter, upprätta och följa upp personuppgiftsbiträdesavtal, ha löpande kontakt med tjänsteleverantören kring systemutveckling, informationshantering och personuppgiftsbehandling, löpande registervård och informationsklassificering av systemet.

Information och anvisningar för hur man ska arbeta i de olika verksamhetssystemen finns på systemsidorna på Insidan. I många fall finns systemadministratörer, systemexperter eller superusers lokalt i verksamheten som ger utbildning och kan hjälpa till med support.

6.4.1 IST – barn- och elevregister

IST är vårt barn- och elevregister. Det utgör själva källdatan till flera andra verksamhetssystem. I det här systemet ska alla de uppgifter finnas som behövs för att identifiera och kontakta de barn och elever, och dess vårdnadshavare, som deltar i vår verksamhet. Det omfattar uppgifter såsom namn, adress, kontaktuppgifter, personnummer och i förekommande fall foto. Härifrån sköts även betygsregistrering och rapportering av olika slag till SCB.

Vänd dig till din skoladministratör eller forskolaskola.systemsupport@kungsbacka.se om du har frågor om IST.

6.4.2 Vklass – pedagogiskt kommunikations- och dokumentationssystem

Vklass är det verksamhetssystem där den huvudsakliga kommunikationen mellan skola och elev och vårdnadshavare ska ske. Det är också här som den pedagogiska dokumentationen och informationen om barns och elevers kunskapsutveckling ska finnas. Här ska uppgifter såsom om kunskapsbedömningar, extra anpassningar, utredning av elevers behov av särskilt stöd och särskilda stödåtgärder som beslutas i form av åtgärdsprogram, underlag från utvecklingssamtal, pedagogisk dokumentation och löpande information till vårdnadshavare finnas.

Vänd dig till din skoladministratör eller forskolaskola.systemsupport@kungsbacka.se om du har frågor om Vklass.

6.4.3 PMO – elevhälsans dokumentationssystem

PMO är det system där elevhälsans gemensamma arbete och de separata professionerna dokumenterar sitt arbete med elever; skolsköterska/skolläkare, skolpsykolog, kurator, specialpedagog och rektor. Här finns dokumentation om både förebyggande, främjande och åtgärdande insatser. Systemet är uppbyggt med hänsyn till rådande sekretessgränser mellan elevhälsans kompetenser och dess samlade elevhälsouppdrag.

I många fall dokumenteras i PMO den eller de djupare utredningar som behövs för att klarlägga en elevs behov av särskilt stöd i någon del (exempelvis skolsocial eller psykologisk utredning), medan den sammanfattande utredningen över behoven kopplat till de pedagogiska målen dokumenteras i Vklass.

6.4.4 Ciceron – vårt diarie- och ärendehanteringssystem

Ciceron är vårt diarie- och ärendehanteringssystem där diarieföring och handläggningen av olika ärenden sker.

Systemet är ett kommungemensamt system men med tydliga myndighetsgränser för respektive nämnd.

Vänd dig till din skoladministratör eller Förskola & Grundskolas centrala Ciceron-administratör om du har frågor om Ciceron. Det finns också information och manualer om Ciceron på Insidan.

6.4.5 Microsoft Office 365 – vårt kommunikations- och samarbetssystem

Microsoft Office 365 (O365) är det kontorsverktyg som vi i Kungsbacka kommun använder för att kommunicera, dela, lagra samt samarbeta kring information med. Både personal och elever har ett personligt konto med tillgång till många verktyg och funktioner inom O365.

Eget arbetsmaterial lagras i första hand i det personliga utrymmet på OneDrive (dokument kan också delas härifrån med kollegor), medan gemensamt arbetsmaterial lagras på en gemensam SharePoint-yta. Office 365 innehåller utöver dessa funktioner även vår e-posthantering genom Outlook. För Förskola & Grundskola har funktionaliteten i Office365 också utökats så att vi kan ta skydd för (kryptera) information av känslig karaktär när vi endera tillfälligt lagrar informationen som eget arbetsmaterial i OneDrive, samarbetar med kollegor för att samla in eller bearbeta information eller överför informationen via e-post. Via Teams inom O365 finns även möjlighet till digitalt samarbete i arbets- eller lärgrupper med möjlighet att under givna villkor fjärrkommunicera.

Läs mer om kryptering och fjärrkommunicering här nedan.

Kryptering

Funktionaliteten att kryptera filer och information är viktig i de fall som det inte går att arbeta med informationen i något av de huvudsakliga verksamhetssystemen, eller

när det är nödvändigt att överföra sådan information via e-post. Krypteringen betyder att vi kan ta skydd för information av känslig karaktär genom att styra villkoren för informationen.

Med känslig information menar vi följande:

1. Information som innehåller *känsliga personuppgifter* enligt dataskyddsförordningen

2. Information som innehåller *extra skyddsvärd eller integritetskänslig information*

3. Information som omfattas av *sekretess*

En viktig begränsning är att inte använda kryptering för information som omfattas av *absolut sekretess*, såsom exempelvis medicinsk information inom elevhälsan. Här gäller uteslutande elevhälsans verksamhetssystem PMO eller i förekommande fall fysisk akt i arkivskåp. Vid ett eventuellt utlämnande med anledning av registerutdrag ska informationen lämnas som utskrifter med rekommenderad post eller expedieras via säker e-postbrevlåda (genom tjänsten Eko-post) om den enskilde så begär det och har en sådan.

Att det systemtekniskt finns möjlighet att ta skydd för känslig information på detta sätt – genom kryptering – innebär dock att det ändå *endast* ska användas i de fall då det inte finns någon annan systemlämplig lösning till buds. Vi ska alltså fortsatt vara mycket varsamma med information av känslig karaktär och endast behandla den information som krävs för uppgiften, och aktivt minska risken för spridning utanför de avsedda verksamhetssystemen.

Exempel på situationer/information där skydd i form av kryptering kan behövas är följande:

- **För att överföra känslig elevinformation via e-post till:**
  - mottagande skola utanför kommunen
  - vårdnadshavare
  - myndighet

När information som är krypterad överförs via e-post kommer mottagaren behöva ett verktyg för att läsa informationen. Om mottagaren inte har ett sådant verktyg får den information om hur den laddar ner ett sådant verktyg för att kunna ta del av informationen. Innan överföring av sådan information via e-post ska man alltid överväga om rekommenderad post är ett alternativ. Det finns också möjlighet att expediera information via säker digital e-postbrevlåda.

I undantagsfall kan informationen överföras via e-post till annan myndighet utan ytterligare kryptering – inom eller utanför Kungsbacka kommuns organisation. Detta eftersom själva överföringen omfattas av kryptering och den mottagande myndigheten är ansvarig för att ta hand om inkommande information.

Glöm inte att ta bort informationen från din utkorg.

- **För att samla in och samarbeta kring analys av information i ett dokument:**
  - insamling och bedömning av undervisande lärares observationer och iakttagelser i syfte att utreda behov av särskilt stöd
  - insamling och bedömning av information för att utreda orsak till en elevs skolfrånvaro
  - insamling och bedömning av information för att utreda kränkningar
  - insamling och bedömning av information för att utreda klagomål på utbildningen
  - insamling och bedömning av information i ordningsärenden

- **För att skydda tillfälligt arbetsmaterial innehållande information av känslig karaktär:**
  - utredningsunderlag av olika slag

För att förebygga att information som skyddas inte tas omhand när behovet av skydd är över kan slumpvisa kontroller göras. Då kontrolleras att dokument som skyddats följer Förskola & Grundskolas namnstandard och att dokumenten inte ligger kvar ohanterade under längre period än nödvändigt.

Du som delar ett dokument med känslig information av något slag med andra i syfte att samla in eller samarbeta kring information av känslig karaktär, ansvarar för att informationen förs över i rätt verksamhetssystem eller tas omhand på annat avsett sätt när arbetet är klart och behovet av skydd därmed inte längre finns. Observera att du måste ta bort dokumentets skydd/kryptering innan du överför det till verksamhetssystemet.

Ta för vana att regelbundet följa upp de ställen där du förvarar krypterat arbetsmaterial och den mapp där du har de dokument som du delat med andra personer.

Efter att informationen eller dokumentet är överfört i rätt verksamhetssystem ska du aktivt radera informationen/dokumentet. Ta för vana att alltid tömma papperskorgen på datorn när du har raderat information/dokument som varit krypteringsskyddade alternativt använd kortkommandot *Shift + Delete* när du raderar dem. Systemadministratören för Office365 kan i särskilda fall återskapa dokument som du raderat av misstag.

Det är viktigt att du är noggrann när du tar skydd för din information så att du klassificerar den ordentligt. Följ de särskilda tillämpningsanvisningar som finns kring kryptering på Insidan och använd knapparna i dokumentets systemvy för att sätta rätt skydd. Fråga hellre en gång för mycket än för lite.

Kontakta Lev Grunberg, utvecklare digitalt lärande stöd
lev.grunberg@kungsbacka.se

Fjärrkommunikation i utbildningen

Behovet av fjärrkommunikation i skolan utgår från elevers rätt till utbildning. Rätten till utbildning omfattar både undervisningen och andra inslag i utbildningen som ingår i utbildningens syfte och som regleras i skollagen och läroplanen.

Behandlingen av personuppgifter som görs i detta sammanhang baseras därmed på någon av de lagliga grunderna allmänt intresse, rättslig förpliktelse eller myndighetsutövning. För fjärrkommunikationen finns rutiner och en teknisk säkerhet som säkerställer hanteringen. Ingen information från själva fjärrkommunikationen – det man pratar om under ett möte – blir åtkomlig för någon utomstående och den sparas inte på något sätt. Information om att man deltagit i möte och användarnamnet sparas dock under en period.

Inom Förskola & Grundskola är det okej att fjärrkommunicera i undervisningen och vid andra inslag i utbildningen som omfattar harmlös information via Teams. För fjärrkommunikation i samband med integritetskänsligare ämnen såsom utvecklingssamtal, särskilt stöd och utredning av kränkande behandling är det bara okej om det inte står andra kommunikationsvägar till buds via till exempel tjänstetelefon eller personligt möte och det även i övrigt bedöms som en lämplig mötesform utifrån vad mötet gäller.

Inom elevhälsans medicinska, psykologiska och psykosociala insats ska Teams tills vidare inte användas alls. Under våren 2021 kommer verktyg för Digitala invånarmöten finnas tillgängligt för elevhälsan och andra liknade mötessammanhang. Verktyget kommer också kunna användas för interna möten och professionsmöten med andra aktörer/myndigheter som exempelvis SIP-möten.

Följ FG:s tillämpningsanvisningar för fjärrkommunikation för att säkerställa din hantering i fjärrsammanhang. Anvisningarna är gemensamma för FG och GA.

7 Incidentrapportering

Personuppgiftsincidenter är händelser där enskilda utsätts för risker på grund av att deras personuppgifter inte skyddas tillräckligt. En personuppgiftsincident uppstår när personuppgifterna som vi behandlar av någon anledning *förstörs*, *förvanskas*, *försvinner* eller *ändras*. Det kan också vara om någon som inte har *behörig tillgång* till personuppgifterna kan *komma åt dem* eller om personuppgifterna på ett obehörigt sätt *röjs*.

Om du som medarbetare inom Förskola & Grundskola får information om en personuppgiftsincident (som uppstått eller riskerar att uppstå) ska du alltid anmäla dessa uppgifter skyndsamt. Med skyndsamt menas helst inom någon timme och absolut senast samma dag som du fick informationen.

Samma rutin gäller oavsett vad det är för typ av personuppgifter och i vilket sammanhang som händelsen skett.

7.1 Sänd anmälan till forskola.grundskola@kungsbacka.se

Anmäl genom att maila till forskola.grundskola@kungsbacka.se . Beskriv vad du har fått reda på utan att röja känsliga, extra skyddsvärda/integritetskänsliga eller sekretessuppgifter om enskilda personer.

Ett stöd för informationen i din anmälan får du om du använder Datainspektionens blankett. Den är hjälpsam för att kartlägga vad som har hänt även om det inträffade inte är av sådan karaktär att händelsen ska anmälas till Datainspektionen. Om det inträffade bedöms som så allvarligt att incidenten är anmälningspliktig så görs det av systemförvaltare/motsvarande eller förvaltningens dataskyddskontakt.

Datainspektionens blankett hittar du på Insidan. Förskola & Grundskolas information om dataskyddsförordningen

7.2 Utredning

När anmälan har tagits emot öppnar registrator ett ärende diarie- och ärendehanteringssystemet Ciceron (Förskola & Grundskolas centrala diarium) där uppgifterna som du har lämnat handläggs och bedöms av systemförvaltare eller motsvarande. Uppgifterna kan behöva kompletteras från dig och/eller andra som kan ha information om det som hänt.

Du som anmäler uppgifterna kontaktas alltid för att verifiera ärendet och för att du ska veta att uppgifterna utreds och tas omhand.

Om du är systemförvaltare eller motsvarande för ett verksamhetssystem eller annan digital tjänst där personuppgifter hanteras ska du utreda de anmälda uppgifterna i det aktuella ärendet i Ciceron. För din utredning och bedömning kan du använda det

utredningsstöd som finns framtaget för ändamålet. Det finns också en mer detaljerad beskrivning av utredningsprocessens olika steg. Du hittar det via länken

Personuppgifter inom Förskola & Grundskola

Om det krävs åtgärder i verksamhetssystem som FG själv inte är systemägare för, utan där Digitalt Center behöver hjälpa till med att antingen verifiera eller radera information, låsa konto eller på annat sätt hindra otillåten spridning av information via enskilda användares konton (elevkonto eller personalkonto) ska förvaltningschef snarast kontaktas för att göra en begäran om det. Förvaltningschefens godkännande behövs för att Digitalt Center ska kunna bistå i ärendet. Bakgrunden är att det bara är högsta förvaltningsledningen som kan begära att få del av information i ett skol-/tjänstekonto och det måste vara väl underbyggt att ett ingrepp i skol-/tjänstekontot är nödvändigt. De enskilda som berörs måste naturligtvis också involveras.

Därefter läggs ett ärende till Digitalt Center i Artwise där omständigheterna beskrivs och vad informationen/åtgärden behövs för samt att ärendet omfattas av lagbundna skyndsamhetskrav. Information kan behövas för att utreda personuppgiftsincident men kan också behövas för att utreda och motverka kränkningar och vidta ordningsåtgärder. Kränknings- och ordningsärenden ska alltid anmälas och utredas via rektor i särskild ordning. Personuppgiftsincidenter kan dock anmälas direkt via till förvaltningsbrevlådan forskola.grundskola@kungsbacka.se.

Kom ihåg att det alltid är en prioriterad uppgift att utreda, bedöma och åtgärda personuppgiftsincidenter. Det betyder att andra arbetsuppgifter kan komma att behöva skjutas fram i tiden. Tala med din närmaste chef för att vid behov få stöd att göra prioritering.

7.3 Åtgärda

Om utredningen visar att de registrerades integritet har åsidosatts, eller riskerar att åsidosättas i samband med vår verksamhet, ska åtgärder vidtas för att ställa situationen till rätta.

Om riskerna innebär allvarlig skada för en eller flera registrerade ska incidenten anmälas till Datainspektionen inom 72 timmar. (Detta görs av systemförvaltare eller motsvarande beroende på var incidenten uppstått.) En allvarlig skada kan till exempel vara att någon förlorat kontrollen över sina uppgifter eller att en registrerad individs rättigheter inskränks med följdverkningar såsom diskriminering, identitetstöld, finansiell förlust eller brott mot sekretess. Om detta har hänt ska den registrerade också få information om detta och om anmälan, om det inte är obehövligt.

Det är systemförvaltare eller motsvarande funktion för digitala tjänster/verktyg/verksamhetsprocess som bedömer och i förekommande fall anmäler personuppgiftsincidenter vidare till Datainspektionen, samt vidtar de åtgärder som krävs. Det kan handla om allt från att initiera systemutveckling till att göra rensningar av manuella konton, skärpa rutiner eller förbättra användarinformation.

Förskola & Grundskolas dataskyddskontakt ska i normalfallet konsulteras vid bedömning av incident och anpassning av åtgärd och läggas till för kännedom i varje förekommande ärende. Om dataskyddsombudet behöver konsulteras ansvarar dataskyddskontakten för att bereda det. Anmälan till Datainspektionen och den fastställda utredningen expedieras av registrator till kommunstyrelsens förvaltning och dataskyddsombud.

7.4 Anmäl delegationsbeslut till nämnd

Uppgiften att utreda och besluta om åtgärder med anledning av en personuppgiftsincident är delegerad till förvaltningschef med vidaredelegering till systemförvaltare eller motsvarande funktion med ansvar för andra digitala tjänster/verktyg/process, se Förskola & Grundskolas delegeringsförteckning. Det betyder att meddelande om delegationsbeslut ska skickas för varje enskilt ärende till nämnden för Förskola & Grundskola. Det gör du genom att döpa din utredning till ”Delegeringsbeslut [delegeringsnr] – utredning och beslut PUI [verksamhetssystem]”.

Prata med registrator eller Förskola & Grundskolas centrala systemadministratör för Ciceron fö om du behöver hjälp att anmäla delegeringsbeslut.

Se vidare Förskola & Grundskolas processbeskrivning för hantering av personuppgiftsincidenter.

8 Rutin vid begäran om registerutdrag, återkallande av samtycke m.m.

Enskilda har som tidigare nämnts rätt att begära registerutdrag över vilka personuppgifter som vi inom Förskola & Grundskola behandlar om henne eller honom, och/eller rättelse av personuppgifter. Den registrerade har också rätt att begära att bli bortglömd, återta samtycke, invända eller begränsa behandling av personuppgifter eller begära att få uppgifterna i ett sådant format att de kan användas i till exempel en annan it-miljö.

Alla sådana begäranden görs via kommunens hemsida https://www.kungsbacka.se/Kommun-och-politik/dataskydd/dina-rattigheter/

Förskola & Grundskola följer de kommungemensamma rutinerna för alla dessa ärenden. Det betyder att när vi inom Förskola & Grundskola får en sådan begäran prövas och samordnas den av Förskola & Grundskolas dataskyddskontakt, och den eller de funktioner som berörs kontaktas för eventuella utdrag.

Handläggningen av en begäran ska normalt ta högst 30 dagar. Om du blir kontaktad i samband med en sådan begäran betyder det alltså att uppgiften är prioriterad och du förväntas hjälpa till med den information eller åtgärd som behövs.

Om begäran gäller registerutdrag kontaktas i första hand den registerbeskrivningsansvarige eller systemförvaltare för att göra personsökning och utdrag i det aktuella registret. Som medarbetare inom Förskola & Grundskola ska vi dock alltid vara beredda på att lämna information som vi eventuellt har om den registrerade i register som sträcker sig till arbetsytor utanför de centrala verksamhetssystemen. I ett registerutdrag ska all information där den registrerade förekommer i med sina personuppgifter lämnas. Om dokumenten är relativt likartade, exempelvis betygshandlingar eller lönespecifikationer, kan den senaste handlingen lämnas med information om att ytterligare liknande handlingar finns att tillgå i registret. Arkiverat material och arbetsmaterial lämnas som regel dock inte i ett registerutdrag.

Registerutdraget ska lämnas tillsammans med en översikt som visar under vilka omständigheter som uppgifterna behandlas. Det finns ett särskilt formulär som ska användas för detta. Det ifyllda formuläret lämnas tillsammans med själva utdraget från registren genom handräckning av fysiska utskrifter till Förskola & Grundskolas huvudregistrator. Registratorn expedierar sedan materialet i den form som den registrerade önskat. Om den som begärt utdraget har anmält en säker digital brevlåda ska utdraget expedieras dit. I annat fall ska utdraget expedieras med rekommenderad post.

Om personuppgifterna omfattar känsliga personuppgifter/uppgifter som omfattas av sekretess expedieras registerutdraget från Förskola & Grundskola, exempelvis om det omfattar utdrag från skolhälsovårdsjournal. I annat fall expedieras utdraget

samlat från kommunledningskontoret. Registratorn ombesörjer att underlaget från Förskola & Grundskolas register i så fall expedieras dit.

Se vidare Förskola & Grundskolas processbeskrivning och dokumentationsmallar som finns i avsett SharePoint-rum eller tillhandahålls av dataskyddskontakt.

9 Tjänsteleverantörer

Inom Förskola & Grundskola följer vi kommungemensamma rutiner när det gäller upprättande av avtal kring personuppgiftshantering med tjänsteleverantörer, så kallade personuppgiftsbiträdesavtal (PUB-avtal). Det betyder att Förskola & Grundskola ansvarar för att upprätta PUB-avtal med sådana leverantörer som i kommunen enbart levererar tjänster till Förskola & Grundskola. För upprättande av sådana avtal ska SKL:s dokumentmall användas. Denna mall finns här: https://skl.se/ekonomijuridikstatistik/juridik/offentlighetsekretessarkiv/dataskyddsforordningengdpr/informationsinsatserkringdataskyddsforordningen/personuppgiftsbitrade.16046.html

Avtalet ska förberedas och följas upp av systemförvaltare eller motsvarande som är kontaktperson gentemot leverantören. I samband med avtalsupprättandet ska behandlingen även kontrolleras mot Förskola & Grundskolas förteckning över personuppgiftsbehandlingar så att beskrivningen av behandlingen och PUB-avtalet överensstämmer med vartannat. Systemförvaltare eller motsvarande ansvarar för att kontakta dataskyddkontakt för att upprätta eller justera beskrivningen över behandlingen i förteckningen.

Var noggrann med instruktionsbilagan i avtalet och använd den checklista som tagits fram för att gå igenom att avtalet har med rätt delar. Checklistan finns i FG:s Sharepointrum för dataskydd eller kontakta dataskyddskontakt (Kolla dataskyddet > Kolla PUB-avtalet).

Avtalet ska föredras och undertecknas av förvaltningschef och därefter registreras Ciceron. Be registrator om hjälp att öppna ett ärende för dig.

I de fall som tjänsteleverantörens egen standardmall för Pub-avtal har använts, ska en alltid en förklaring biläggas i ärendet som visar att avtalet motsvarar de krav som ställs på sådana avtal. Exempelvis genom Förskola & Grundskolas checklista för detta.

Förskola & Grundskolas dataskyddskontakt kan användas som stöd för bedömning av PUB-avtal.

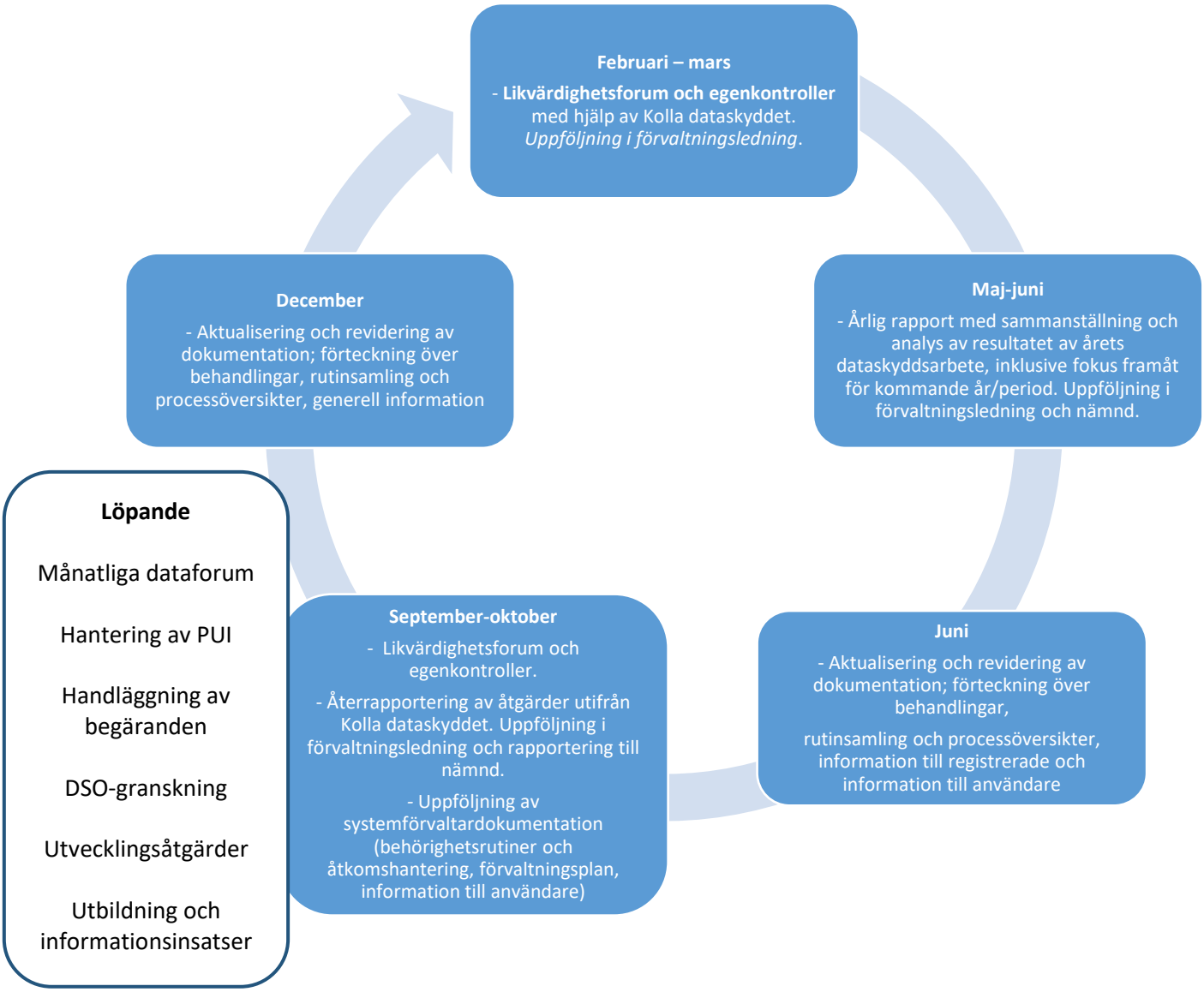
I de fall som flera nämnder omfattas av tjänsteleverantören ska avtalet föredras för och undertecknas av bitr. kommundirektör, och diarieföras i KS diarium.

10 Kvalitetssäkring

En av dataskyddsförordningens grundprinciper handlar om ansvarsskyldighet. Det innebär att bedriva ett systematiskt och dokumenterat kvalitetssäkringsarbete runt hanteringen av personuppgifter i verksamheten som påvisar regelefterlevnaden. En del av det arbetet är den kartläggning och kvalitetssäkring som sker i samband med upprättandet och underhållet av förteckningen över Förskola & Grundskolas personuppgiftsbehandlingar, en annan del är det arbete som sker utifrån de risker och brister som visar sig i personuppgiftsincidenter. En annan del är arbetet som systemförvaltare gör i samband med informationsklassificering och upprättande och uppföljning av PUB-avtal samt dataskyddsombudets oberoende granskningar av verksamhetens arbete. En annan del är arbetet med egenkontroller.

10.1 Årshjul

Dataskyddsarbetet ska på samma sätt som det systematiska arbetsmiljöarbetet och kvalitetsarbetet vara pågående i verksamhetens planering och vardag. Under verksamhetsåret följer arbetet dock i stora drag nedanstående uppföljningar och aktiviteter:


Februari – mars
- Likvärdighetsforum och egenkontroller med hjälp av Kolla dataskyddet. Uppföljning i förvaltningsledning.
Maj-juni
- Årlig rapport med sammanställning och analys av resultatet av årets dataskyddsarbete, inklusive fokus framåt för kommande år/period. Uppföljning i förvaltningsledning och nämnd.
Juni
- Aktualisering och revidering av dokumentation; förteckning över behandlingar,
rutinsamling och processöversikter, information till registrerade och information till användare
September-oktober
- Likvärdighetsforum och egenkontroller.
- Återrapportering av åtgärder utifrån Kolla dataskyddet. Uppföljning i förvaltningsledning och rapportering till nämnd.
- Uppföljning av systemförvaltardokumentation (behörighetsrutiner och åtkomshantering, förvaltningsplan, information till användare)
December
- Aktualisering och revidering av dokumentation; förteckning över behandlingar, rutinsamling och processöversikter, generell information
Löpande
Månatliga dataforum
Hantering av PUI
Handläggning av begäranden
DSO-granskning
Utvecklingsåtgärder
Utbildning och informationsinsatser

11 Organisering och ansvar

11.1 Personuppgiftsansvarig och dataskyddsombud

Ansvarig för verksamhetens personuppgiftsbehandling kallas personuppgiftsansvarig (PUA). I Kungsbacka är det de olika nämnderna som är personuppgiftsansvariga. Som personuppgiftsansvarig ska man utse ett dataskyddsombud (DSO). Ombudets uppgift är vara att bevaka följsamheten mot dataskyddsförordningen, vara kontakt gentemot Datainspektionen och på olika sätt ge råd och stöd i frågor som rör den personuppgiftsansvariges dataskyddsarbete. DSO fungerar också som kontakt för de registrerade vid klagomål. DSO nås på dataskyddskontakt@kungsbacka.se eller 0300-83 40 66.

11.2 Dataskyddskontakt

För det operativa dataskyddsarbetet i verksamheten ska det för varje förvaltning i Kungsbacka finnas en dataskyddskontakt. Dataskyddskontakten har som uppgift att samordna förvaltningens arbete med personuppgiftsfrågor utifrån rådande lagstiftning. Dataskyddskontakten har till uppgift att:

- upprätta förteckning över personuppgiftsbehandlingar över verksamhetens personuppgiftsbehandling och revidera förteckningen vid behov
- samordna och besvara begäran om registerutdrag m fl begäranden från registrerade för den egna verksamheten
- säkra upp att nödvändiga rutiner och instruktioner gällande hantering av personuppgifter finns tillgängliga inom den egna verksamheten
- vara behjälplig med att bedöma om personuppgiftsincidenter behöver vidarerapporteras till Datainspektionen och om de registrerade behöver informeras
- vara förvaltningens representant i det kommunövergripande nätverket för dataskyddskontakter
- vara ett stöd till personuppgiftsansvarig, förvaltningsledningen och verksamheten i arbetet med personuppgiftsfrågor
- uppmärksamma personuppgiftsansvarig och förvaltningsledningen på åtgärder som måste vidtas för att upprätthålla en god hantering av personuppgifter i enlighet med rådande lagstiftning
- vara kommunens Dataskyddsombud behjälplig samt fungera som länk mellan Dataskyddsombud och personuppgiftsansvarig
- omvärldsbevaka kring personuppgiftsfrågor utifrån det egna verksamhetsområdet
- vid behov inhämta råd och stöd från Dataskyddsombud

Kontaktuppgifter till förvaltningens dataskyddskontakt finns på Insidan samt på förvaltningens sidor på kungsbacka.se.

11.3 Systemförvaltare/motsvarande

Inom Kungsbacka används en gemensam modell för systemförvaltning som kallas *systemförvaltarmodellen*. Den innebär att systemförvaltare eller motsvarande såsom systemadministratör på förvaltningsnivå eller ansvarig för ett digitalt verktyg eller tjänst, som en del av systemskötseln ansvarar för att ta hand om och bevaka dataskyddet i sitt/sina system. Konkret betyder det att ansvara för att utreda och åtgärda eventuella personuppgiftsincidenter, vid begäran lämna registerutdrag, upprätta och följa upp personuppgiftsbiträdesavtal, upprätta rutiner för behörighetstilldelning och anvisningar för hur användare ska handskas med personuppgifter i systemet.

Som stöd i arbetet finns förvaltningens dataskyddskontakt.

11.4 Registerbeskrivningsansvarig

Inom Förskola & Grundskola har vi tillfört en roll som vi kallar registerbeskrivningsansvarig. Det är helt enkelt de personer som i sin funktion ansvarar för att underhålla och bevaka eller vara kontaktperson för en viss process för personuppgiftsbehandling. Exempel är mottagande till grundsärskola eller samordna av brukarenkät. Den som är beskrivningsansvarig för en given personuppgiftsbehandling medverkar i arbetet med att underhålla förteckningen över personuppgiftsbehandlingar.

11.5 Medarbetare

Som medarbetare inom Förskola & Grundskola förväntas du på samma sätt som inom andra områden, hålla dig informerad om och följa Förskola & Grundskolas instruktioner kring hanteringen av personuppgifter. Du förväntas genom ditt arbete också indirekt eller direkt bidra till att utbildningens grundläggande värden såsom den personliga integriteten får fäste hos de barn och elever som deltar i vår

verksamhet, samt att utbildningen i praktiken genomförs på ett sätt som tar hänsyn detsamma. Din inställning till hanteringen av personuppgifter betyder mycket för att barn, elever vårdnadshavare och anställda ska känna sig trygga med hur deras personuppgifter handhas inom vår verksamhet.

11.6 Chef

Utöver din roll som medarbetare inom Förskola & Grundskola förväntas du som chef skapa förutsättningar för din personal att lära sig om vad dataskyddsförordningen och respekten för den personliga integriteten betyder i praktiken. Området bör därför behandlas på olika sätt i olika forum såsom vid APT, i värdegrundsarbetet, kvalitetsarbetet, IKT-arbetet och liknande. Du förväntas också hjälpa din personal vidare vid frågor om Förskola & Grundskolas rutiner.

11.7 Förvaltningsledning

Förvaltningsledningen ansvarar för att verkställa dataskyddet i verksamheten och beakta dataskyddet i beslut om har bäring på personuppgiftsbehandling av något slag. Centralt är att hålla sig informerad om dataskyddsfrågor och uppföljningen av regelefterlevnaden, besluta i avgörande frågor och förmedla relevant information vidare i linjen. Utöver egenkontroller görs även uppföljning av hur förvaltningen följer dataskyddsförordningen i samband med DSO:s granskning.

Personuppgiftsbiträdesavtal

Innehållsförteckning

1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER 2
2. DEFINITIONER 3
3. BAKGRUND OCH SYFTE 4
4. BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION 4
5. DEN PERSONUPPGIFTSANSVARIGES ANSVAR 4
6. PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN 5
7. SÄKERHETSÅTGÄRDER 5
8. SEKRETESS/TYSTNADSPLIKT 6
9. GRANSKNING, TILLSYN OCH REVISION 6
10. HANTERING AV RÄTTELSER OCH RADERING M.M. 7
11. PERSONUPPGIFTSINCIDENTER 7
12. UNDERBITRÄDE 8
13. LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND 9
14. ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING 9
15. LAGVAL OCH TVISTLÖSNING 9
16. PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING 9
17. ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M. 9
18. ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE 10
19. MEDDELANDEN INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER 10
20. KONTAKTPERSONER 11
21. ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER 11
22. PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET 11

PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt Allmänna dataskyddsförordningen EU 2016/679, art. 28.3[1]

1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	**Personuppgiftsbiträde**
Förskola & Grundskola, Kungsbacka Gymnasium & Arbetsmarknad, Kungsbacka Kultur & Fritid, Kungsbacka	IST AB
Organisationsnummer	**Organisationsnummer**
212000-1256	556265-4755
Postadress	**Postadress**
Vägmästaren, Syréngatan 1, 434 43 Kungsbacka	Ingelstadsvägen 9, 352 34 VÄXJÖ
Kontaktperson för administration av detta personuppgiftsbiträdesavtal	**Kontaktperson för administration av detta personuppgiftsbiträdesavtal**
Namn: Simon Englén E-post: simon.englen@kungsbacka.se Tfn: 0300-83 41 73	Namn: Oscar Burman E-post: oscar.burman@ist.com Tfn: 0470 70 71 00
Kontaktperson för parternas samarbete om dataskydd	**Kontaktpersoner för parternas samarbete om dataskydd**
För Förskola & Grundskola: Namn: Karin Malmsten E-post: karin.malmsten@kungsbacka.se Tfn: 0300-83 55 65 För Gymnasium & Arbetsmarknad: Namn: Markus Ternblad E-post: markus.ternblad@kungsbacka.se Tfn: 0300-83 41 66 För Kultur & Fritid: Namn: Pia Burwall E-post: pia.burwall@kungsbacka.se Tfn: 0300-83 46 65	Namn: Oscar Burman E-post: Oscar.burman@ist.com Tfn: 0470 70 71 00

[1] Allmänna dataskyddsförordningen EU 2016/679 föreskriver att det ska finnas ett skriftligt avtal om Personuppgiftsbiträdets Behandling av Personuppgifter för Den personuppgiftsansvariges räkning.

AS

2. DEFINITIONER

Utöver de begrepp som definieras i löptext, i detta personuppgiftsbiträdesavtal, ska dessa definitioner oavsett om de används i plural eller singular, i bestämd eller obestämd form, ha nedanstående innebörd när de anges med versal som begynnelsebokstav.

Behandling	En åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättningar av Personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
Dataskyddslagstiftning	Avser all integritets- och personuppgiftslagstiftning, samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter), som är tillämplig på den personuppgiftsbehandling som sker enligt detta PUB-avtal, inklusive nationell sådan lagstiftning och EU-lagstiftning.
Personuppgiftsansvarig	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för Behandlingen av Personuppgifter.
Instruktion	De skriftliga instruktioner som närmare anger föremål, varaktighet, art och ändamål, typ av Personuppgifter samt kategorier av Registrerade och särskilda behov som omfattas av Behandlingen.
Logg	Logg är resultatet av Loggning.
Loggning	Loggning är ett kontinuerligt insamlande av uppgifter om den Behandling av Personuppgifter som utförs enligt detta PUB-avtal och som kan knytas till en enskild fysisk person.
Personuppgiftsbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning.
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de Personuppgifter som överförts, lagrats eller på annat sätt Behandlats.
Registrerad	Fysisk person vars Personuppgifter Behandlas.
Tredje land	En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till Europeiska ekonomiska samarbetsområdet (EES).

Underbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som i egenskap av underleverantör till Personuppgiftsbiträdet Behandlar Personuppgifter för Personuppgiftsansvariges räkning.

3. BAKGRUND OCH SYFTE

3.1 Med detta Personuppgiftsbiträdesavtal ("PUB-avtalet") reglerar den Personuppgiftsansvarige Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige. PUB-avtalets syfte är att säkerställa den Registrerades fri- och rättigheter vid Behandlingen, i enlighet med vad stadgas i Allmänna dataskyddsförordningen EU 2016/679 ("Dataskyddsförordningen"), art. 28.3.

3.2 PUB-avtalet utgör ett självständigt avtal om Behandlingen. När PUB-avtalet utgör ett av flera avtalsdokument inom ramen för ett annat avtal benämns det andra avtalet "Huvudavtalet" i PUB-avtalet.

3.3 För det fall något av det som stadgas i kap. 1, 16, 17, 18.2, 19 – 22 i PUB-avtalet regleras på annat sätt i Huvudavtalet ska Huvudavtalets reglering ha företräde.

3.4 PUB-avtalets information, i form av bestämmelser och andra uppgifter som påverkar PUB-avtalets tillämpning, samt PUB-avtalets hänvisningar till sådan information, t.ex. lagstiftning (inklusive förordningar och föreskrifter), avser vid var tid gällande sådan information.

4. BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION

4.1 Den Personuppgiftsansvarige utser härmed Personuppgiftsbiträdet att utföra Behandlingen för den Personuppgiftsansvariges räkning enligt vad som stadgas i detta PUB-avtal.

4.2 Den Personuppgiftsansvarige ska ge Instruktioner till Personuppgiftsbiträdet om hur det ska utföra Behandlingen.

4.3. Personuppgiftsbiträdet får endast utföra Behandlingen i enlighet med PUB-avtalet och vid var tid gällande Instruktioner.

5. DEN PERSONUPPGIFTSANSVARIGES ANSVAR

5.1 Den Personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för Behandlingen och för att utforma korrekta Instruktioner så att Personuppgiftsbiträdet och Underbiträdet kan fullgöra sitt eller sina uppdrag enligt detta PUB-avtal och Huvudavtal i förekommande fall.

5.2 Den Personuppgiftsansvarige ska utan onödigt dröjsmål informera Personuppgiftsbiträdet om förändringar i Behandlingen vilka påverkar Personuppgiftsbiträdets skyldigheter enligt Dataskyddslagstiftningen.

AS

5.3 Den Personuppgiftsansvarige ansvarar för att informera Registrerade om Behandlingen och för att tillvarata Registrerades rättigheter enligt Dataskyddslagstiftningen samt vidta varje annan åtgärd som åligger den Personuppgiftsansvarige enligt Dataskyddslagstiftningen.

6. PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN

6.1 Personuppgiftsbiträdet förbinder sig att endast utföra Behandlingen i enlighet med PUB-avtalet och Instruktioner samt att följa Dataskyddslagstiftningen. Personuppgiftsbiträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.

6.2 Personuppgiftsbiträdet ska vidta åtgärder för att skydda Personuppgifterna mot alla slag av Behandlingar som inte är förenliga med PUB-avtalet, Instruktioner och Dataskyddslagstiftningen.

6.3 Personuppgiftsbiträdet åtar sig säkerställa att samtliga fysiska personer som arbetar under dess ledning följer PUB-avtalet och Instruktioner samt att de fysiska personerna informeras om relevant lagstiftning.

6.4 Personuppgiftsbiträdet ska på begäran från den Personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt Dataskyddsförordningen, art. 32-36, fullgörs och svara på begäran om utövande av den Registrerades rättigheter i enlighet med Dataskyddsförordningen, kap. III, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå.

6.5 För det fall att Personuppgiftsbiträdet finner att Instruktioner är otydliga, i strid med Dataskyddslagstiftningen eller saknas och Personuppgiftsbiträdet bedömer att nya eller kompletterande Instruktioner är nödvändiga för att genomföra sina åtaganden ska Personuppgiftsbiträdet utan dröjsmål informera den Personuppgiftsansvarige, tillfälligt upphöra med Behandlingen och invänta nya Instruktioner.

6.6 För det fall att den Personuppgiftsansvarige förser Personuppgiftsbiträdet med nya eller ändrade Instruktioner ska Personuppgiftsbiträdet, utan onödigt dröjsmål från mottagandet, meddela den Personuppgiftsansvarige huruvida genomförandet av de nya Instruktionerna föranleder förändrade kostnader för Personuppgiftsbiträdet.

7. SÄKERHETSÅTGÄRDER

7.1 Personuppgiftsbiträdet ska vidta alla tekniska och organisatoriska säkerhetsåtgärder som krävs för att förhindra Personuppgiftsincidenter, genom att säkerställa att Behandlingen uppfyller kraven i Dataskyddsförordningen och att den Registrerades rättigheter skyddas.

7.2 Personuppgiftsbiträdet ska fortlöpande säkerställa att den tekniska och organisatoriska säkerheten i samband med Behandlingen medför en lämplig nivå av konfidentialitet, integritet, tillgänglighet och motståndskraft.

7.3 Eventuella tillkommande eller ändrade krav på skyddsåtgärder från den Personuppgiftsansvarige, efter parternas tecknande av PUB-avtalet, ska betraktas som nya Instruktioner enligt PUB-avtalet.

7.4 Personuppgiftbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbiträdets ledning och som behöver åtkomsten för att kunna utföra sina arbetsuppgifter.

7.5 Personuppgiftsbiträdet åtar sig att kontinuerligt Logga åtkomst till Personuppgifterna enligt PUB-avtalet i den utsträckning det krävs enligt Instruktionen. Loggar får gallras först fem (5) år efter Loggningstillfället om inte annat anges i Instruktionen. Loggar ska omfattas av erforderliga skyddsåtgärder, i enlighet med Dataskyddslagstiftningen.

7.6 Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa Behandlingens säkerhet.

8. SEKRETESS/TYSTNADSPLIKT

8.1 Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska vid Behandlingen iaktta såväl sekretess som tystnadsplikt. Personuppgifterna får inte nyttjas eller spridas för andra ändamål, vare sig direkt eller indirekt, såvida inte annat avtalats.

8.2. Personuppgiftsbiträdet ska tillse att samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen, är bundna av sekretessförbindelse avseende Behandlingen. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag. Personuppgiftsbiträdet åtar sig även att tillse att det finns sekretessavtal med Underbiträdet samt sekretessförbindelser mellan Underbiträdet och samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen.

8.3 Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om eventuella kontakter med tillsynsmyndighet avseende Behandlingen. Personuppgiftsbiträdet har inte rätt att företräda den Personuppgiftsansvarige eller agera för den Personuppgiftsansvariges räkning gentemot tillsynsmyndigheter i frågor avseende Behandlingen.

8.4 Om den Registrerade, tillsynsmyndighet eller tredje man begär information från Personuppgiftsbiträdet vilken rör Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om saken. Information om Behandlingen får inte lämnas till den Registrerade, tillsynsmyndighet eller tredje man utan skriftligt medgivande från den Personuppgiftsansvarige, såvida det inte framgår av tvingande lag att information ska lämnas. Personuppgiftsbiträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller lagkrav.

9. GRANSKNING, TILLSYN OCH REVISION

9.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål, på den Personuppgiftsansvariges begäran, tillhandahålla den information om tekniska och organisatoriska säkerhetsåtgärder som den Personuppgiftsansvarige behöver för att kunna fastställa att Personuppgiftsbiträdet uppfyller sina åtaganden enligt PUB-avtalet och Dataskyddsförordningen, art. 28.3 h.

9.2 Personuppgiftsbiträdet åtar sig att minst en (1) gång om året granska säkerheten avseende Behandlingen genom en egenkontroll för att säkerställa att Behandlingen följer PUB-avtalet. Resultatet av sådan egenkontroll ska på begäran delges den Personuppgiftsansvarige.

AB

9.3 Den Personuppgiftsansvarige äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till Personuppgiftsbiträdet), följa upp att Personuppgiftsbiträdet uppfyller PUB-avtalets, Instruktionernas och Dataskyddslagstiftningens krav. Personuppgiftsbiträdet ska vid sådan granskning bistå den Personuppgiftsansvarige, eller den som utför granskningen i den Personuppgiftsansvariges ställe, med dokumentation, tillgång till lokaler, IT-system och andra tillgångar som behövs för att kunna granska Personuppgiftsbiträdets efterlevnad av PUB-avtalet, Instruktioner och Dataskyddslagstiftningen. Den Personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastade sekretess eller tystnadsplikt enligt lag eller avtal.

9.4 Personuppgiftsbiträdet äger alternativt till vad som stadgas i punkterna 9.2-9.3, rätt att erbjuda andra tillvägagångssätt för granskning av Behandlingen, exempelvis granskning genomförd av oberoende tredje part. Den Personuppgiftsansvarige ska i sådant fall äga rätt, men inte skyldighet, att tillämpa detta alternativa tillvägagångssätt för granskning. Vid sådan granskning ska Personuppgiftsbiträdet ge den Personuppgiftsansvarige eller en tredje part den assistans som behövs för utförandet av granskningen.

9.5 Personuppgiftbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning, även om sådan tillsyn annars skulle stå i strid med bestämmelserna i PUB-avtalet.

9.6 Personuppgiftsbiträdet ska tillförsäkra den Personuppgiftsansvarige rättigheter gentemot Underbiträdet vilka motsvarar den Personuppgiftsansvariges samtliga rättigheter gentemot Personuppgiftsbiträdet enligt kap. 9 i PUB-avtalet.

10. HANTERING AV RÄTTELSER OCH RADERING M.M.

10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbiträdets felaktiga Behandling ska Personuppgiftsbiträdet vidta lämplig åtgärd utan onödigt dröjsmål, senast inom trettio (30) dagar, från det att Personuppgiftsbiträdet mottagit erforderlig information från den Personuppgiftsansvarige. När den Personuppgiftsansvarige begärt radering får Personuppgiftsbiträdet endast utföra Behandling av den aktuella personuppgiften som ett led i processen för radering.

10.2 Om tekniska och organisatoriska åtgärder (t.ex. uppgraderingar eller felsökningar) vidtas av Personuppgiftsbiträdet i Behandlingen, vilka kan väntas påverka Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige skriftligt om detta i enlighet med vad stadgas om meddelanden i 19 kap. i PUB-avtalet. Informationen ska lämnas i god tid innan åtgärderna vidtas.

11. PERSONUPPGIFTSINCIDENTER

11.1 Personuppgiftsbiträdet ska ha förmåga att återställa tillgängligheten och tillgången till Personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt Dataskyddsförordningen, art. 32.1 c.

11.2 Personuppgiftbiträdet åtar sig att med beaktande av Behandlingens art, och den information som Personuppgiftsbiträdet har att tillgå, bistå den Personuppgiftsansvarige med att fullgöra dennes

skyldigheter vid en Personuppgiftsincident beträffande Behandlingen. Personuppgiftbiträdet ska på den Personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörigs Behandling och/eller åtkomst till Personuppgifterna.

11.3 Vid Personuppgiftsincidenter, vilka Personuppgiftbiträdet fått vetskap om, ska Personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta den Personuppgiftsansvarige om händelsen. Personuppgiftsbiträdet ska med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå tillhandahålla den Personuppgiftsansvarige en skriftlig beskrivning av Personuppgiftsincidenten.

Beskrivningen ska redogöra för:

1. Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet Registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
2. de sannolika konsekvenserna av Personuppgiftsincidenten, och
3. åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra Personuppgiftincidentens potentiella negativa effekter.

11.4 Om det inte är möjligt för Personuppgiftsbiträdet att tillhandahålla hela beskrivningen samtidigt, enligt punkt 11.3 i PUB-avtalet, får beskrivningen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

12. UNDERBITRÄDE

12.1 Personuppgiftsbiträdet ansvarar fullt ut för Underbiträdets Behandling gentemot den Personuppgiftsansvarige.

12.2 Personuppgiftsbiträdet äger rätt att anlita ett nytt underbiträde. När Personuppgiftsbiträdet avser att anlita ett nytt underbiträde ska Personuppgiftsbiträdet säkerställa underbiträdets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om

1. underbiträdets namn, organisationsnummer och säte (adress och land),
2. vilken typ av uppgifter och kategorier av Registrerade som behandlas, och
3. var Personuppgifterna ska behandlas.

12.3 Personuppgiftsbiträdet äger rätt att upphöra med att anlita Underbiträdet. När Personuppgiftsbiträdet upphör med att anlita Underbiträdet ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om att det upphör med att anlita Underbiträdet.

12.4 Personuppgiftsbiträdet åtar sig att teckna ett skriftligt personuppgiftsbiträdesavtal med det nya underbiträdet och säkerställa att det nya underbiträdet åläggs samma skyldigheter som Personuppgiftsbiträdet åläggs enligt detta PUB-avtal.

12.5 Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran översända en kopia av det personuppgiftsbiträdesavtal som Personuppgiftsbiträdet tecknat med Underbiträdet.

12.6 Den Personuppgiftsansvarige äger inom 30 dagar rätt att invända mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde och att, med anledning av sådan invändning, säga upp detta PUB-avtal att upphöra i enlighet med vad stadgas i PUB-avtalet, punkt 17.4.

AS

13. LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

13.1 Personuppgiftsbiträdet ska säkerställa att Personuppgifterna hanteras och lagras inom EU/EES av en fysisk eller juridisk person som är etablerad inom EU/EES, om inte PUB-avtalets parter kommer överens om något annat.

13.2 Personuppgiftsbiträdet äger endast rätt att överföra Personuppgifter till Tredje land för Behandling (t.ex. service, support, underhåll, utveckling, drift eller liknande hantering) om den Personuppgiftsansvarige på förhand skriftligen godkänt sådan överföring och utfärdat Instruktioner för detta ändamål.

13.3 Överföring till Tredje land för Behandling enligt PUB-avtalet, punkt 13.2, får endast ske om den är förenlig med Dataskyddslagstiftningen och uppfyller de krav på Behandlingen vilka ställs i PUB-avtalet och Instruktioner.

14. ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING

14.1 Vid ersättning för skada i samband med Behandling som, genom fastställd dom eller förlikning, ska utgå till den Registrerade på grund av överträdelse av bestämmelse i PUB-avtalet, Instruktioner och/eller tillämplig bestämmelse i Dataskyddslagstiftningen ska art. 82 i Dataskyddsförordningen tillämpas.

14.2 Sanktionsavgifter enligt Dataskyddsförordningen, art. 83, eller Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 6 kap. 2 § ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.

14.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

14.4 Oaktat vad sägs i Huvudavtalet gäller detta PUB-avtal, punkter 14.1 och 14.2, före andra regler om fördelning mellan Parterna av krav sinsemellan såvitt avser Behandlingen.

15. LAGVAL OCH TVISTLÖSNING

För detta avtal gäller svensk rätt. Eventuell tolkning eller tvist i anledning av PUB-avtalet, som parterna inte kan lösa på egen hand, ska avgöras av svensk allmän domstol.

16. PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING

16.1 PUB-avtalet gäller från och med den tidpunkt PUB-avtalet undertecknats av båda parter och tillsvidare. Parterna äger ömsesidig rätt att säga upp PUB-avtalet att upphöra med trettio (30) dagars varsel.

17. ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.

17.1 Endera part i PUB-avtalet äger rätt att påkalla omförhandling av PUB-avtalet om motpartens ägarförhållanden ändras väsentligt eller om tillämplig lagstiftning, eller tolkningen av den, ändras på

ett för Behandlingen avgörande sätt. Påkallande av omförhandling enligt första meningen innebär inte att PUB-avtalet till någon del upphör att gälla utan endast att en omförhandling om PUB-avtalet ska påbörjas.

17.2 Tillägg till, och ändringar i, PUB-avtalet ska vara skriftliga och undertecknade av båda parter.

17.3 När någon av parterna får kännedom om att motparten agerar i strid med PUB-avtalet, Instruktioner och/eller Dataskyddslagstiftningen, ska parten utan dröjsmål meddela motparten om agerandet. Därefter äger parten rätt att med omedelbar verkan upphöra att utföra sina förpliktelser enligt PUB-avtalet till den tidpunkt motparten förklarat att agerandet upphört och förklaringen accepterats av den part som påtalat agerandet.

17.4 Om den Personuppgiftsansvarige invänder mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde, enligt detta PUB-avtal, punkt 12.6, har den Personuppgiftsansvarige rätt att säga upp PUB-avtalet att upphöra med omedelbar verkan. Om Personuppgiftsbiträdet Behandlar Personuppgifterna efter den tidpunkt som anges i punkt 18.2 gäller vad stadgas i punkter 18.3-18.4.

18. ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE

18.1 Vid uppsägning av PUB-avtalet ska den Personuppgiftsansvarige utan onödigt dröjsmål begära att Personuppgiftsbiträdet överlämnar samtliga Personuppgifter till den Personuppgiftsansvarige eller raderar dem, enligt dennes önskemål. Om Personuppgifterna överlämnas ska det ske i ett öppet och standardiserat format. Med samtliga Personuppgifter avses alla Personuppgifter vilka har omfattats av Behandlingen samt annan tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt PUB-avtalet.

18.2 Överlämning och radering enligt PUB-avtalet, punkt 18.1, ska vara utförda senast trettio (30) dagar räknat från den tidpunkt uppsägning gjorts enligt detta PUB-avtal, punkt 16.1

18.3 Behandling som utförs av Personuppgiftsbiträdet efter den tidpunkt som stadgas i punkt 18.2 är att betrakta som en otillåten Behandling.

18.4 Bestämmelser om sekretess/tystnadsplikt i 8 kap. PUB-avtalet ska fortsätta gälla även om PUB-avtalet i övrigt upphör av gälla.

19. MEDDELANDEN INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER

19.1 Meddelanden om PUB-avtalet och dess administration inklusive uppsägning ska skickas till respektive parts kontaktperson för PUB-avtalet.

19.2 Meddelanden om parternas samarbete om dataskydd, gällande Behandlingen, ska skickas till respektive parts kontaktperson för parternas samarbete om dataskydd.

19.3 Meddelanden inom ramen för PUB-avtalet och Instruktioner ska skickas skriftligt. Ett meddelande ska anses ha kommit fram till mottagaren senast en (1) arbetsdag efter att meddelandet har skickats.

20. KONTAKTPERSONER

20.1 Parterna ska utse var sin kontaktperson för PUB-avtalet.

20.2 Parterna ska utse var sin kontaktperson för parternas samarbete om dataskydd.

21. ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER

21.1 Varje part ansvarar för att de uppgifter som anges i 1 kap. i PUB-avtalet alltid är aktuella. Ändring av uppgifter i 1 kap. ska meddelas skriftligt enligt punkt 19.1 i PUB-avtalet.

22. PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET

22.1 Detta PUB-avtal tillhandahålls antingen i digitalt format för elektroniskt tecknande eller i pappersformat för tecknande med penna. Om PUB-avtalet tillhandahålls i digitalt format utgår punkter 22.2-22.3.

22.2 Den Personuppgiftsansvariges undertecknande av PUB-avtalet

Ort Kungsbacka Datum 2019-11-04

.....

Undertecknande

Anneli Skoglund

.....

Namnförtydligande

22.3 Personuppgiftsbiträdets undertecknande av PUB-avtalet

Ort Växjö Datum 9/10-19

.....

Undertecknande

Andreas Fröcklin

.....

Namnförtydligande

Mall för den Personuppgiftsansvariges Instruktion för Behandling av Personuppgifter

Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet även följa nedanstående Instruktion:

1. Ändamål, föremålet och arten

IST används som barn och elevregistersystem inom Förskola & Grundskola, Gymnasium & Arbetsmarknad och Kultur & Fritid. I systemet behandlas personuppgifter för en rad olika ändamål med gemensamt syfte att tillhandahålla utbildning och verksamhet inom respektive verksamhetsområde. Elevregistret med tillhörande typer av personuppgifter används även för verksamhetsnära behandlingar knutna till den löpande verksamheten.

Gemensamt för FG, KFT och GA:s behandlingar är att verifiera barn, elever, dess vårdnadshavare och administrera kontaktuppgifter för anställda. Gemensamt är även att administrera placering, gruppering och klassindelning i syfte att planera, organisera och fördela resurser i samband med verksamheten (exempelvis modersmålsundervisning, skolskjuts, praktik, studie- och yrkesvägledning, elevpeng).

Inom FG och GA behandlas även personuppgifter i syfte att administrera betygsättning och provresultat på nationella ämnesprov samt rapportera rapporteringspliktig statistik till myndigheter och andra instanser såsom SCB, gymnasieantagning m. fl.

Inom FG och KFT behandlas personuppgifter även i syfte att fakturera vårdnadshavare för barnomsorg respektive kulturskola.

Respektive nämnd är personuppgiftsansvarig för den behandling som utförs i systemets respektive verksamhetsdelar.

2. Behandlingarna omfattar följande typer av Personuppgifter

I systemet hanteras följande typer av personuppgifter för barn/elever och dess vårdnadshavare samt anställda:

- Förnamn
- Efternamn
- Personnummer
- Telefonnummer
- Mejladress
- Folkbokföringsadress och alternativ/tillfällig adress

För elever hanteras utöver dessa uppgifter även följande typer av personuppgifter:

- Grupp/Klasstillhörighet
- Placering
- Uppgift om rätt till modersmålsundervisning/studiehandledning på modersmålet

3. Behandlingen omfattar kategorier av Registrerade

- Anställda (Lärare, rektorer, administratörer m. fl.)

AS

- Elever/Förskolebarn
- Vårdnadshavare

4. Särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena

Behandling av personuppgifter får, från tid till annan, inkludera:
Upprätta fjärråtkomst till den Personuppgiftsansvariges system för att undersöka, assistera och åtgärda tekniska problem.
Behandla supportärenden, samtal och andra supportförfrågningar från den Personuppgiftsansvarige.
Installation, uppdatering och konfigurering av programvara samt systemintegrationer.
Överföring av databas (dumpar/filer) med Personuppgifter till Personuppgiftsbiträdets IT-miljö för felsökning eller konvertering. Dessa data ska raderas efter utfört uppdrag.
Drift av Personuppgiftsansvariges IT-miljö eller tillhandahållande av Molntjänster innehållande Personuppgifter.
Behöver personuppgifterna behandlas på annat sätt än vad som här anges ska Personuppgiftsbiträdet inhämta godkännande från Personuppgiftsansvarig.

Personuppgiftsansvarig bestämmer gallringstiderna och utför gallring för personuppgifter. Personuppgiftsbiträdet utför endast gallring efter uttrycklig instruktion från Personuppgiftsansvarig.

5. Särskilda tekniska och organisatoriska säkerhetsåtgärder vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena

Biträdet ska uppfylla de krav som anges utifrån den Personuppgiftsansvariges informationsklassning samt redovisa status för dessa på begäran.

6. Särskilda krav på Loggning vad gäller Behandling av Personuppgifter samt vilka som ska ha tillgång till dem

Personuppgiftsbiträdet och Underbiträden ska ansvara för att:

I de fall arbete utförs i Personuppgiftsansvariges miljö med personuppgifter gäller att:

I Personuppgiftsbiträdets system logga väsentliga händelser som:

Inloggning i Personuppgiftsansvariges miljö, med uppgifter om när, av vem, varför och på vems uppdrag samt vilka åtgärder som skett.

Om Personuppgiftsdata överförts till Personuppgiftbiträdet skall anledningen till detta anges och vem hos Personuppgiftsansvarige som beställt detta anges.

När uppdraget är slutfört skall det loggas och eventuella överförda Personuppgiftsdata raderas.

Personuppgiftsansvarig äger rätt att göra stickprovskontroller av dessa loggar.

Att teknisk åtkomstloggning utförs och dess detaljeringsgrad är Personuppgiftsansvariges ansvar. Exempel på teknisk automatisk åtkomstloggning är vem som loggat in i systemet och när, vilka åtgärder som skett med uppgifter om en registrerad person.

I de fall Personuppgiftsbiträdet driftar system eller tillhandahåller molntjänster med Personuppgifter åt Personuppgiftsansvarig gäller att: Loggning av väsentliga händelser och teknisk åtkomstloggning sker i enighet med specifikation i leveransavtalet för respektive drift och molntjänst.
7. Lokalisering och överföring av Personuppgifter till Tredje land
Personuppgiftsbiträdet får inte överföra den Personuppgiftsansvariges Personuppgifter till tredje land såvida inte dokumenterade instruktioner från den Personuppgiftsansvarige givits om detta.
8. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av biträdet/biträdena
Personuppgiftsbiträdet ska lämna ut loggar till den personuppgiftsansvarige endast i xml-format om detta avtal upphör att gälla.

Förteckning över Underbiträden vid PUB-avtalets ingående

Nedan anges i vilka situationer som Personuppgiftsbiträdet uppdragit till ett underbiträde att för Personuppgiftsbiträdets räkning behandla personuppgifter. Inom parentes anges de länder där respektive bolag är etablerat och från vilka personal kan komma att Behandla Personuppgifter för Personuppgiftsbiträdets räkning.

- Ex. Personuppgiftsbiträdet Limited (Storbritannien)
- Ex. Personuppgiftsbiträdet (Irland)

Versionshantering

Version	Datum	Förändringar	Ansvarig
1	2019-04-24		SE

Kungsbacka

Fjärrkommunikation i utbildningen

Så gör vi inom grundskolan och gymnasieskolan

Sammanställt 2020-06-05

Innehåll

Fjärrkommunikation via Teams i utbildningen 3
Personuppgifter 3
Generellt 3
Frågor? 4
Undervisning 5
Det här gäller 5
Tänk på det här 5
Generellt 6
Guider 6
Andra inslag i utbildningen 7
Det här gäller 7
Tänk på det här 7
Särskilda samtal 9
Det här gäller 9
Tänk på det här 9
Elevhälsa - skolsköterskas, psykologs och kurators insats 11
Det här gäller 11
Tänk på det här 11
Guider 12
Så här gör du för att skapa en aktivitet/inbjudan i Teams: 12
A. Inbjudan via Teams 12
B. Inbjudan via Teams kalender 13
C. Inbjudan via Teams Chatt 14
Läs mer 14
Begränsa inspelningsmöjligheter 15
A. Före mötet 15
B. Under mötet 15
Läs mer 16

Fjärrkommunikation via Teams i utbildningen

Som ett sätt att hjälpa elever som i enlighet med Folkhälsomyndighetens rekommendationer eller av annan tillfällig omständighet inte kan följa undervisningen i skolan har vi möjlighet att bedriva undervisning och annan utbildningsrelaterad verksamhet på distans.

Det kan ske antingen i realtid (fjärrkommunikation när elever och lärare inte är åtskilda i tid men i rum) eller på distans (när elever och lärare är åtskilda i både tid och rum). Den här informationen berättar om vad som gäller och vad man ska tänka på.

I dokumentet ”Information till rektorer i grundskolan” 2020-05-18 finns mer information om vad du som rektor ska tänka på när det gäller fjärr- och distansundervisning i grundskolan med anledning av den nya förordningen. Använd gärna informationen i bilagorna till detta dokument för att informera föräldrar och elever.

Personuppgifter

Behovet av fjärrkommunikation inom grundskolan och gymnasieskolan utgår från elevers rätt till utbildning. Rätten till utbildning omfattar både undervisningen och andra inslag i utbildningen som ingår i utbildningens syfte och som regleras i skollagen och läroplanen. Behandlingen av personuppgifter som görs i detta sammanhang baseras därmed på någon av de lagliga grunderna *allmänt intresse*, *rättslig förpliktelse* eller *myndighetsutövning*. För fjärrkommunikationen finns rutiner och en teknisk säkerhet som säkerställer hanteringen. Ingen information från själva fjärrkommunikationen – det man pratar om under ett möte – blir åtkomlig för någon utomstående och den sparas inte på något sätt. Information om *att* man deltagit i möte och användarnamnet sparas dock under en period.

Inom FG och GA är det okej att fjärrkommunicera i undervisningen och vid andra inslag i utbildningen som omfattar harmlös information via Teams. För fjärrkommunikation i samband med integritetskänsligare ämnen såsom utvecklingssamtal, särskilt stöd och utredning av kränkande behandling är det bara okej om det inte står andra kommunikationsvägar till buds via till exempel telefon (via teleoperatör) eller personligt möte och det även i övrigt bedöms som en lämplig mötesform utifrån vad mötet gäller. Inom elevhälsans medicinska, psykologiska och psykosociala insats ska Teams inte användas alls. Detta kan komma att förändras beroende på resultatet av pågående arbete för att säkerställa förutsättningarna för detta.

Generellt

- ✓ Följ kommunens regler för informationssäkerhet (exempelvis lösenordspolicy) och var vaksam på avvikelser. Inled aldrig en kommunikation med någon som du inte först verifierat genom röst och video.
- ✓ Anmäl eventuella incidenter som du är med om till forskolagrundskola@kungsbacka.se eller gymnasiumocharbetsmarknad@kungsbacka.se. Beskriv vad som hänt, när det hände hur man kan komma i kontakt med dig för mer information.
- ✓ Upplever du problem med fjärrkommunikationen kommer du under hösten 2020 att kunna få support via Service direkts webbanmälan och 4444. Tills vidare vänder du dig till din lokala IKT-pedagog eller respektive stödfunktion inom din förvaltning.

Frågor?

Har du frågor som rör Teams i utbildningen eller om riktlinjer för undervisning om och användning av digitala verktyg i lärandet, vänd dig till Lev Grunberg, Åsa Blide Larsson (FG) eller Andreas Logg (GA).

Har du frågor som rör Teams inom elevhälsans område, vänd dig till Åsa Bergström, medicinsk verksamhetschef.

Har du frågor som rör dataskydd och integritet går det bra att vända dig till förvaltningarnas dataskyddskontakter Karin Malmsten (FG) eller Markus Ternblad (GA).

Undervisning

Det här gäller

Fjärrkommunikation i undervisningen går bra och verktyget vi ska använda för det är Teams. Följ anvisningarna nedan och läs mer på Insidan om hur du använder Teams i lärandet. På www.skolahemma.se finns inspiration och tips om undervisning via fjärr- och/eller distans.

Tänk på det här

- ✓ Ta först ställning till om fjärrkommunikation i undervisningen är bästa sättet för eleven att följa med i undervisningen, eller om det finns andra sätt. Om lektionen handlar om enskild, tyst läsning kan det vara mer effektivt att ha kontakt med eleven på annat sätt.
- ✓ I Kungsbacka har vi gjort bedömningen att elever från 12 års ålder kan delta i undervisning via fjärrkommunikation, förutsatt att eleven har fungerande utrustning som den är van att arbeta med i skolan. Utgångpunkten för bedömningen är skolornas förstärkta arbete kring kunskap och träning i digitala verktyg. För yngre elever och elever inom grundsärskolan och gymnasiesärskolan krävs att man hittar ett annat upplägg för undervisningen eller säkrar upp med stöd via förälder eller annat vuxenstöd.
- ✓ Fokusera på lärarledda genomgångar vid fjärrkommunikationen. Undvik mindre strukturerad verksamhet såsom grupparbeten. Undvik att ”fjärra” situationer och aktiviteter där du inte har kontroll på vilka som kommer befinna sig i rummet.
- ✓ Skapa aktiviteten genom något av alternativen längre ned i detta dokument. Låt bara de elever som deltar hemifrån samt läraren och eventuell gästföreläsare vara deltagare i mötet.
- ✓ Utgångspunkten är att fjärrkommunikation via Teams inte ska spelas in. Det finns dock situationer där inspelningsfunktionen måste kunna användas i undervisningen, exempelvis vid ”flippade” undervisningssituationer. Om du som lärare ska spela in vissa sekvenser i undervisningen är det viktigt att du innan informerar och säkerställer att elever som deltar på distans stänger av mikrofon och kamera. Filmen finns tillgänglig i Team-aktiviteten i 20 dagar.

  Observera att elever aldrig ska ingå i inspelade sekvenser i Teams som skolan initierar.

  Observera även att du som mötesarrangör själv måste begränsa inspelningsmöjligheten manuellt när du skapar aktiviteten. Det gör du genom att i själva Teams-aktiviteten gå till ”Mötesalternativ” och sedan välja att bara du kan presentera. Då kan ingen annan än du starta kameran. Följ anvisningarna nedan.

- ✓ Om vårdnadshavare önskar delta på en lektion via elevens uppkoppling genom att sitta jämte, uppmana dem att höra av sig till dig som lärare före. Informera om att de som digitala besökare ska vara beredda på att presentera sig på samma sätt som fysiska besökare och att eventuella frågor eller synpunkter om lektionens upplägg ska tas upp i efterhand med läraren eller rektorn och inte under lektionen.
- ✓ Externa deltagare (exempelvis gästföreläsare) kommer under hösten 2020 att behöva autentisera sig med BankId eller motsvarande. Tills dess ska bekräftade e-postadresser användas när externa deltagare deltar.
- ✓ Placera kameran så att elever som är i det fysiska klassrummet inte exponeras mer än nödvändigt och att elever som distraheras av fjärrkommunikationen inte sitter nära. Säkerställ framför allt att elever med skyddade personuppgifter inte syns eller hörs i fjärrkommunikationen.

- ✓ **Innan lektionsstart** – kontrollera att eleverna som deltar på distans kommer in i Teams-rummet och kan interagera via påslagen kamera och ljud.
- ✓ **Vid lektionsstart** – välkomna alla, både elever på distans och elever på plats, och klargör förutsättningarna för lektionen, exempelvis att lektionen inte får spelas in och att man ska sitta i ett enskilt utrymme där man kan fokusera.
  Gör klart vilka "spelregler" som gäller - räck upp handen när du vill ha ordet, kommunicera via chatten till alla (informera om att chatten bara ska användas för det digitala samarbetet såsom att ställa fråga eller meddela teknikproblem och information av harmlös karaktär), ha mikrofonen avstängd när du inte har ordet.
- ✓ **Under lektionen** – Ha koll på chatten, vem som räcker upp handen och i vilken ordning elever begärt ordet. Ha koll på att elever på distans hänger med i undervisningen och att du har kontakt med dem. Håll uppsikt så att ingen annan sköter kommunikationen via din dator.
- ✓ **Efter lektionen** – kontrollera att fjärrkommunikationen avslutas.
- ✓ Filma aldrig elever via Teams. Om underlag för bedömning behövs i form av film (exempelvis hemkunskap, idrott, muntlig framställan) – be eleverna själva filma och lämna in filmfilen via Vklass eller genom att dela filen med dig från OneDrive.

Generellt

- ✓ Elever bör helst inte ha profilbild i O365 miljön, av integritetsskäl. Om elever vill använda profilbild, uppmuntra att använda en profilbild som inte är ett foto. En egen Emojie me-bild kan vara ett alternativ som stödjer igenkänning mellan elever och personal.

Guider

- Hur du schemalägger ett möte i Teams
- Hur du begränsar inspelningsfunktionen

Andra inslag i utbildningen

Med andra inslag i utbildningen menas sådana inslag som inte är undervisning men är en del av utbildningen. Till exempel skolavslutning och föräldramöte.

Det här gäller

För andra inslag i utbildningen såsom skolavslutning, student, föräldramöten och forum för samråd gäller att dessa kan genomföras via Teams, för att elever som inte är i skolan ska kunna ta del. När det gäller skolavslutning och student kan även vårdnadshavare vara motiverade deltagare för att stärka banden mellan hem och skola.

Fjärrkommunikation vid andra inslag i utbildningen som berör mer harmlös information går också bra och verktyget vi ska använda för det är Teams. Följ anvisningarna nedan och läs mer på Insidan om hur du använder Teams.

Tänk på det här

- ✓ Placera kameran så att elever och personal med skyddade personuppgifter inte exponeras. Begränsa även exponeringen av elever och personal vad gäller närbilder och olämpliga vinklar. Se till att personer med skyddade personuppgifter får information om ”sändningen” och förstärk uppsikten så att personerna inte av misstag hamnar i kamerans öga.
  ”Fotograf” och kamera ska vara tydligt utmärkta, exempelvis med gul väst (fotografen) så att det blir lätt för dem som inte vill att välja plats att vara på för att inte vara hamna i bild under fjärrkommunikationen.
- ✓ Vid föräldramöte kan det vara lämpligt att begränsa deltagargruppen till mindre grupper och ha flera möten istället för ett stort.
- ✓ Skapa aktiviteten genom något av alternativen längre ned i detta dokument. Låt bara de elever som deltar hemifrån samt läraren och eventuell gästföreläsare vara deltagare i mötet.
- ✓ Utgångspunkten är att fjärrkommunikation via Teams inte ska spelas in. Det finns dock situationer där inspelningsfunktionen måste kunna användas i vid andra inslag i utbildningen, exempelvis vid generell information till föräldrar. Om du som mötesarrangör ska spela in vissa sekvenser i aktiviteten är det viktigt att du innan informerar och säkerställer att elever, vårdnadshavare och eventuella externa som deltar på distans stänger av mikrofon och kamera. Filmen finns tillgänglig i Team-aktiviteten i 20 dagar. Observera att elever (och vårdnadshavare) aldrig ska ingå i filmade sekvenser i Teams som skolan initierar.

Observera att du som mötesarrangör själv måste begränsa inspelningsmöjligheten manuellt när du skapar aktiviteten. Det gör du genom att i själva Teams-aktiviteten gå till ”Mötesalternativ” och sedan välja att bara du kan presentera. Då kan ingen annan än du starta kameran. Följ anvisningarna nedan.

- ✓ Externa deltagare såsom vårdnadshavare kommer under hösten 2020 att behöva autentisera sig med BankId eller motsvarande. Tills dess ska bekräftade e-postadresser i Vklass användas vid inbjudan när vårdnadshavare deltar.
- ✓ Utse en person som har i uppdrag att sköta mötestekniken, släppa in deltagarna via lobbyn och pricka av att bara inbjudna deltagare släpps in (via en vidarebefordrad länk kan nämligen andra ansluta till mötet) samt styra funktioner i mötet såsom ljud, handuppräckning/frågor och chatt under aktiviteten.

- ✓ Vid mötets start– klargör syftet och förutsättningarna för mötet (se nedan) och kontrollera att deltagarna sitter på ett bra ställe. Informera om att chatten inte är till för att ta anteckningar från mötet och att ingen information ska delas där. Chatten ska bara användas för information av generell karaktär. Informera även om att det som sägs och syns under fjärrkommunikation inte sparas utan det enda som sparas är *att* man medverkat samt användardata (såsom användarnamn). Informationen ska även lämnas i aktivitetens inbjudningstext.
- ✓ Informera deltagarna om att använda påslagen kamera och mikrofon under fjärrkommunikationen, i vart fall vid kommunikationens start utifrån mötesetikett och transparens i kommunikationen. Det kan i vissa fall dock vara nödvändigt att be deltagarna att stänga av kamera och mikrofon under fjärrkommunikationen för att undvika rundgång eller störningar.

- ✓ Informera vårdnadshavare och elever som deltar på fjärr om reglerna för deltagandet:

  - att välja en avskild och neutral placering i rummet eller använda bakgrundsdiffusering
  - fotoförbud på skolan innebär även foto-/inspelningsförbud via fjärrkommunikation. Observera att fjärrkommunikationen inte får spelas in av skolan heller.

- ✓ Nedanstående text kan användas i inbjudan:

  Välkomna till … Syftet med mötet är att … Inbjudna till mötet är vårdnadshavare till elever i klassen/skolan … Under mötet ber vi dig stänga av ljudet för att förhindra rundgång. Behåll kameran påslagen så att alla ser vilka som deltar, om inte mötesarrangören uppmanar att ha den avstängd under mötet. Det som sägs och syns under fjärrkommunikation sparas inte. Det enda som sparas är att man medverkat i mötet samt användardata (såsom användarnamn). Vi ber dig respektera att inte spela in kommunikationen under mötet. Vi vill också upplysa om att chatten som finns bara ska användas för att meddela mötesarrangören eventuella teknikproblem eller dela generell information. Välj en neutral plats att delta från.

  Läs mer om hur Kungsbacka kommun behandlar personuppgifter i utbildningen på kungsbacka.se/Utbildning-och-barnomsorg / https://www.kungsbacka.se/Utbildning-och-barnomsorg/Gymnasieskolor/behandling-av-personuppgifter-i-gymnasium--arbetsmarknad/.

Särskilda samtal

Fjärrkommunikation vid utvecklingssamtal, studie- och yrkesvägledningssamtal och samtal av annan integritetskänslig karaktär. Exempelvis samtal i samband med kränkande behandling, skolfrånvaro och särskilt stöd.

Det här gäller

I första hand bör fysiska möten eller telefon användas framför fjärrkommunikation via Teams. Om det med anledning av rådande omständigheter inte står andra möjligheter till buds, och det även i övrigt bedöms som en ändamålsenlig mötesform utifrån karaktären på mötet, elevens ålder, tillgång till digitala verktyg och andra påverkande omständigheter såsom rum och relation, kan dock Teams-möten användas utifrån anvisningarna här nedan. Detta bygger på att personal och elever redan är kända för varandra.

Tänk på det här

- ✓ Ta först en kontakt med eleven och dess vårdnadshavare och stäm av om det känns ok att ha ett digitalt möte. Personer med skyddade personuppgifter ska som regel inte delta i digitala möten via Teams alls. Stäm av mot respektive handlingsplan om kommunikation via Teams är ok.
- ✓ Om vårdnadshavare önskar delta på en lektion via elevens uppkoppling genom att sitta jämte, uppmana dem att höra av sig till dig som lärare före. Informera om att de som digitala besökare ska vara beredda på att presentera sig på samma sätt som fysiska besökare och att eventuella frågor eller synpunkter om lektionens upplägg ska tas upp i efterhand med läraren eller rektorn och inte under lektionen.
- ✓ Skapa aktiviteten genom något av alternativen längre ned i detta dokument. Låt bara de elever som deltar hemifrån samt läraren och eventuell gästföreläsare vara deltagare i mötet.
- ✓ Fjärrkommunikation via Teams i sammanhang där integritetskänsligare information ska avhandlas ska aldrig spelas in. Observera att du som mötesarrangör själv måste begränsa inspelningsmöjligheten manuellt när du skapar aktiviteten. Det gör du genom att i själva Teams-aktiviteten gå till ”Mötesalternativ” och sedan välja att bara du kan presentera. Då kan ingen annan än du starta kameran. Följ anvisningarna nedan.
- ✓ Externa deltagare (exempelvis gästföreläsare) kommer under hösten 2020 att behöva autentisera sig med BankId eller motsvarande. Tills dess ska bekräftade e-postadresser användas när externa deltagare deltar.
- ✓ Markera mötet som ”Privat” i Outlook. Då kan ingen annan använda anslutningslänken och se vem/vilka som bjudits in till mötet.
- ✓ Vid mötets start– klargör syftet och förutsättningarna för mötet (se nedan) och kontrollera att deltagarna sitter på ett bra ställe. Informera om att chatten inte är till för att ta anteckningar från mötet och att ingen information ska delas där. Chatten ska bara användas för information av generell karaktär. Informera även om att det som sägs och syns under fjärrkommunikation inte sparas utan det enda som sparas är *att* man medverkat samt användardata (såsom användarnamn). Informationen ska även lämnas i aktivitetens inbjudningstext.
- ✓ Informera deltagarna om att använda påslagen kamera och mikrofon under fjärrkommunikationen för transparens i kommunikationen. Det kan i vissa fall dock vara nödvändigt att be deltagarna att stänga av kamera och/eller mikrofon under fjärrkommunikationen för att undvika rundgång eller störningar.

- ✓ Informera deltagarna om reglerna för deltagandet:
  - att välja en avskild och neutral placering i rummet eller använda bakgrundsdiffusering

- att inte på något sätt spela in fjärrkommunikation. Observera att fjärrkommunikationen inte får spelas in av skolan heller.

✓ Nedanstående text kan användas i inbjudan:

> *Välkomna till … Syftet med mötet är att … Håll kamera och ljud påslaget under mötet så att alla ser och hör dem som deltar. Det som sägs och syns under fjärrkommunikation sparas inte. Det enda som sparas är att man medverkat i mötet samt användardata (såsom användarnamn). Vi ber dig respektera att inte spela in kommunikationen under mötet. Vi vill också upplysa om att chatten som finns bara ska användas för att meddela mötesarrangören eventuella teknikproblem eller dela generell information. Välj en neutral plats att delta från.*
>
> *Läs mer om hur Kungsbacka kommun behandlar personuppgifter i utbildningen på kungsbacka.se/Utbildning-och-barnomsorg* / https://www.kungsbacka.se/Utbildning-och-barnomsorg/Gymnasieskolor/behandling-av-personuppgifter-i-gymnasium--arbetsmarknad/.

✓ Eventuell dokumentation från samtalet ska antecknas i avsett verksamhetssystem, exempelvis PMO, Vklass eller Ciceron.

✓ Följ informationen omkring det arbete som pågår för att undersöka möjliga verktyg för att kunna ha digitala möten inom detta område på regelbunden basis.

Elevhälsa - skolsköterskas, psykologs och kurators insats

Det här gäller

Utgångspunkten i nuläget är att samtal inom elevhälsans medicinska, psykologiska och psykosociala insats (exempelvis hälsosamtal, psykologutredning, skolsocial utredning) inte ska ske via Teams alls. Bakgrunden är det höga integritetsskydd som omfattar dessa samtal och insatser, vilket kräver både högt tekniskt skydd men också rumsligt och relationellt. Samtal bör i första hand ske genom bokat möte på skolan eller tjänstetelefon.

I nuläget pågår ett kartläggande arbete för att utvärdera olika tekniska lösningar samt erfarenheter i övrigt när det gäller integritetskänsliga samtal på distans för att på sikt omhänderta värdet av digital elevhälsa.

Tänk på det här

- ✓ Följ informationen omkring det arbete som pågår för att undersöka möjliga verktyg för att kunna ha digitala möten inom elevhälsan när det gäller hälsosamtal och utredningar hos psykolog och kurator.
- ✓ Följ kommunens regler för informationssäkerhet (exempelvis lösenordspolicy) och var vaksam på avvikelser. Inled aldrig en kommunikation med någon som du inte först verifierat genom röst och video.
- ✓ Om elever tar kontakt via Teams, verifiera genom röst och video att det är rätt person samt föreslå att samtalet istället sker på annat sätt via till exempel telefon (med teleoperatör) eller personligt möte om det handlar om elevhälsans medicinska, psykologiska och psykosociala insats (exempelvis hälsosamtal, psykologutredning, skolsocial utredning).
- ✓ Anmäl incidenter som du är med om till forskolagrundskola@kungsbacka.se eller gymnasiumocharbetsmarknad@kungsbacka.se. Beskriv vad som hänt, när det hände hur man kan komma i kontakt med dig för mer information.

Guider

Så här gör du för att skapa en aktivitet/inbjudan i Teams:

Det finns tre olika sätt att bjuda in till ett Teams-möte:

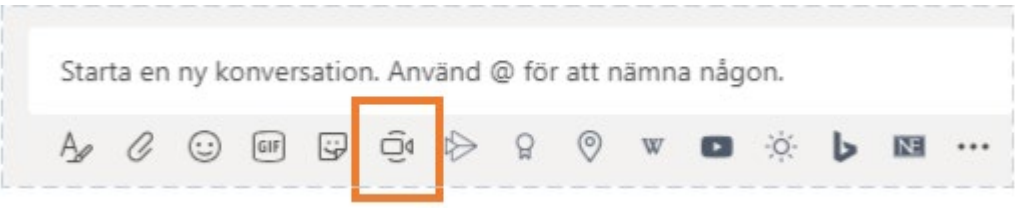
A. Inbjudan via Teams **Allmänt** eller **Kanal**:
B. Inbjudan via Teams **kalender**
C. Inbjudan via Temas **Chatt**

A. Inbjudan via Teams

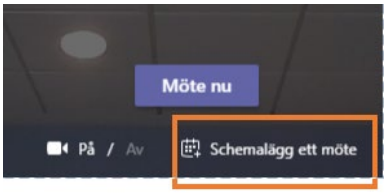
Att schemalägga Teams möte.

Tänk på att alla medlemmar som är inbjudna till Teamet kommer att få inbjudan till mötet. För att få en överblick över vilka som är inbjudna till Teamet gå till **Hantera Team – Medlemmar.**

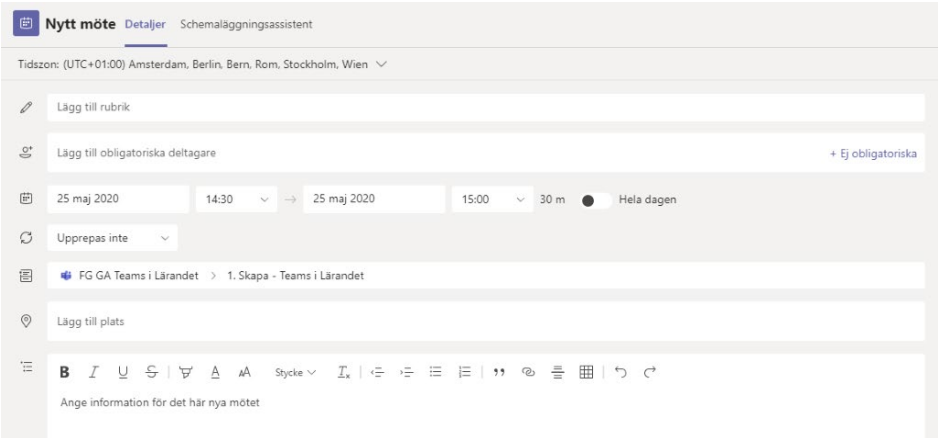
1. Klicka på ikonen kameran vid konversationer under **Allmänt** eller i en **kanal**



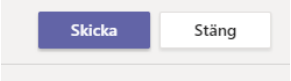
2. Klicka på **Schemalägg ett möte**



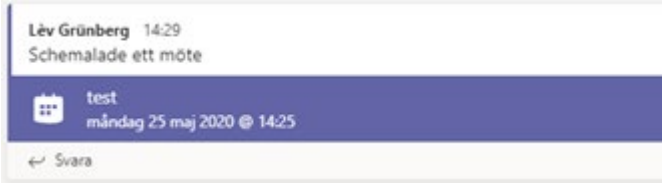
3. Nytt möte:
   a. börja med att skriva en rubrik. Observera att inte ange personuppgifter i mötesrubriken
   b. Du behöver inte lägga till deltagare då du redan har deltagarna i Teamet det vill säga (**Ej obligatorisk)**
   c. Välj datum och tid
   d. Upprepa händelsen vid behov
   e. Hoppa över plats
   f. beskriv vad mötet kommer att behandla



4. Klicka på Skicka längst upp till höger



5. En inbjudan kommer nu att vissas i kommentarsfältet

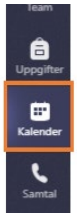


6. Alla medlemmar kommer att få en påminnelse samt att mötet har påbörjats när mötet och nu möjlighet att **Ansluta** till mötet

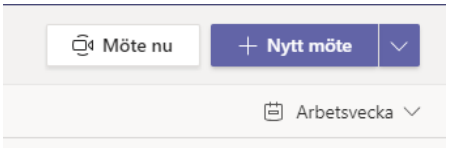
7. Alla kan även se inbjudan direkt i sin Outlook kalender och kan ansluta till mötet. Markera mötet som ”Privat” i Outlook om mötet rör känsligare information

B. Inbjudan via Teams kalender

1. Klicka på kalender ikonen till vänster om Teams



2. Klicka på knappen **+Nytt möte** längst upp till höger alternativt dubbelklicka på en position i kalendern

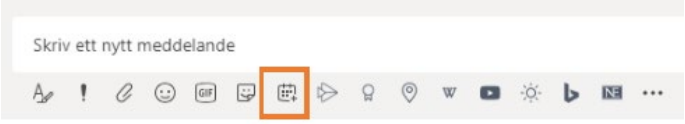


3. Se vidare guiden A. Inbjudan via Teams **punkt 3.**

C. Inbjudan via Teams Chatt

1. Klicka på **Chat** ikonen till vänster om Teams

2. Under konversationsfältet klicka på ikonen kalender



3. Se vidare guiden A. Inbjudan via Teams **punkt 3**

Läs mer

Mer information kring hur du schemalägger möte i Teams hittar du under Microsoft officiella hemsida. Läs mer…

Begränsa inspelningsmöjligheter

Ändra mötesinställningar så att endast den som skapat mötet kan:

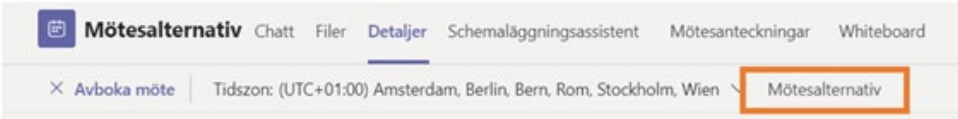
- spela in
- stänga av mikrofonen
- dela innehåll
- ta bort deltagare
- släppa in folk från lobbyn
- ändra roller för andra deltagare

Skapa möte i kalender eller direkt i ett Team

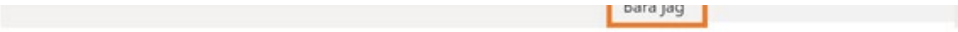
A. Före mötet

1. Gå in på den skapade mötesinbjudan i Teams kalender

2. Välj *Mötesalternativ*



3. Välj *Vem kan presentera – Bara jag*



B. Under mötet

1. Välj *Visa deltagarlista*

2. Välj *Hantera behörigheter*

3. Välj *Vem kan presentera – Bara jag*

Läs mer

Microsoft Ändra mötesalternativ före mötet

Microsoft Ändra mötesalternativ under mötet

Läs även här hur du gör för att styra behörighetsroller https://support.microsoft.com/sv-se/office/roller-i-ett-teams-m%c3%b6te-c16fa7d0-1666-4dde-8686-0a0bfe16e019?ui=sv-se&rs=sv-se&ad=se

Datum
2021-09-01

Dnr
2021-00863

Kungsbacka

Till följande nämnder och bolag:
Förskola & Grundskola, Gymnasium & Arbetsmarknad, Teknik, Miljö & hälsoskydd, Byggnadsnämnden, Vård & Omsorg, Individ & Familjeomsorg, Kommunstyrelsen, Service, Tempohus, Eksta

Regelbunden granskning hösten 2021

Nu startar jag den regelbundna granskningen av nämndernas och bolagens dataskyddsarbete i Kungsbacka kommun. Granskningen kommer att genomföras under oktober–november månad men redan under september önskar jag få del av dokumentation från respektive verksamhet.

Så här kommer granskningen gå till

Granskningen kommer dels bygga på en genomgång av dokumenterade rutiner, information och beskrivningar av dataskyddsarbetet. Dels kommer informationsinhämtning ske genom en muntlig avstämning med verksamhetens GDPR-samordnare och förvaltningschef/VD utifrån de områden som ingår i granskningen.

Tidpunkt för muntlig avstämning meddelas genom separat kalenderbokning.

Rapportering av granskningens resultat

Efter genomförd granskning kommer jag lämna en skriftlig rapport till den nämnd eller styrelse som är personuppgiftsansvarig för verksamheten. En samlad rapport över granskningens resultat på kommunnivå kommer även lämnas till kommunstyrelsen.

Muntlig rapportering erbjuds självfallet till respektive nämnd och styrelse.

Välkommen med frågor om granskningen!

Karin Malmsten,

Dataskyddsombud

Bilaga 1: Informationsinhämtning för regelbunden granskning 2021

Bifoga eller länka till följande dokumentation, i den mån den finns. I den mån ni bedömer att dokumentationen omfattas av sekretess går det bra att lämna den på annat sätt. Kontakta mig i dessa fall.

Senast den 24 september 2021 behöver informationen ha kommit in till dataskyddsombud@kungsbacka.se.

1) Ert **register över personuppgiftsbehandlingen.**
2) Er nämnds/styrelses **delegering när det gäller dataskydd.**
3) Er **information till medarbetarna om vad GDPR och dataskydd innebär.**
4) Exempel på era **anvisningar till medarbetarna** om hur de ska handskas med personuppgifter i er verksamhet – om ni har andra eller kompletterande anvisningar till personalen än de kommungemensamma instruktionerna och anvisningarna.
5) Exempel på er **information till registrerade** om hur ni behandlar personuppgifter och vilka rättigheter de har – om ni har kompletterande eller annan information än den kommungemensamma informationen på kommunens hemsida.
6) Exempel på **information till registrerade** som ni ger i samband med insamlande av personuppgifter (till exempel i samband med ansökningsblankett/e-tjänst).
7) Exempel på era **rutiner för att handlägga registrerades rättigheter** vid begäran om till exempel registerutdrag, radering och rättelse.
8) Exempel på **personuppgiftsbiträdesavtal inkl. instuktionsbilaga** med något av er verksamhets mest centrala personuppgiftsbiträden.
9) Exempel på **avtal vid gemensamt personuppgiftsansvar** i det fall ni har delat ansvar med till exempel en annan nämnd.
10) Exempel på era **rutiner för att ta hänsyn till dataskydd vid upphandling** av nya digitala verktyg, tjänster eller verksamhetssystem.
11) **Årshjul eller liknande planering** för er verksamhets dataskyddsarbete.
12) Er senaste **dokumentation av egenkontroll** som ni gjort på dataskyddsområdet.
13) Er senaste **dokumentation av ledningens genomgång** av dataskydd**.**

Bilaga 2: Om granskningen

En del av dataskyddsombudets uppdrag

Av art. 39 i dataskyddsförordningen framgår att dataskyddsombudet ska ha uppsikt över efterlevnaden av GDPR, de svenska kompletterande dataskyddsbestämmelserna samt den personuppgiftsansvariges strategi för skydd av personuppgifter. En del av detta arbete görs genom att granska respektive nämnds/bolags/stiftelses följsamhet mot GDPR.

Den planerade granskningen för perioden 2021-2022 omfattar *regelbunden granskning* och *fördjupad granskning*. Den regelbundna granskningen omfattar samtliga personuppgiftsansvariga verksamheter i kommunen och är inriktad på verksamheternas dataskyddsarbete i stort[1], medan den fördjupade granskningen görs inom ett avgränsat område som inte per automatik kommer omfatta samtliga verksamheter. Den regelbundna granskningen görs på hösten och den fördjupade granskningen görs på våren.

Läs mer om inriktningen för de olika granskningsformerna och om områdena som ingår i den regelbundna granskningen i *Dataskyddsombudets inriktning och årshjul 2021-2022* (2021-06-29, dnr KS 2021/0313).

Syfte med granskningen

Det övergripande syftet för granskningen är att stimulera till reflektion och lärande omkring den egna verksamhetens dataskyddskapacitet. Med utgångpunkt i granskningen ges råd och rekommendationer som dels kan bidra till att bibehålla och stärka dataskyddet i verksamheten, dels omhänderta eventuella avvikelser. Ett aktivt dataskyddsarbete innebär en stor trygghet för dem vars personuppgifter som verksamheten hanterar.

[1] Mindre omfattande verksamheter är undantagna i 2021 års regelbundna granskning till fördel för andra insatser inom ramen för dataskyddsombudets råd och stöd.