



IT- och digitaliseringsenheten
Bengtsfors, Färgelanda och Åmål

Regler för digital informationshantering

Beslutat av: Kommunstyrelsen

Datum: Den 3 juni 2026, § 106, dnr KS 2026–00184

Dokumentets giltighet: År 2026–2030

Dokumentet gäller för: Kommunkoncernen i sin helhet

Dokumentansvarig: IT- och digitaliseringsenheten
Bengtsfors, Färgelanda och Åmål

IT- och digitaliseringsenheten

Regler för digital informationshantering

i Bengtsfors-, Färgelanda- och Åmåls kommun

Syfte

Kommuners information är en av organisationens allra värdefullaste och känsligaste tillgångar. Medarbetaren behöver ha tillgång till rätt information för att utföra sitt uppdrag på ett effektivt och säkert sätt.

Invånare och brukare måste kunna lita på att deras uppgifter är säkra och bara delas med den som har rätt att se den. Dagens moderna AI-verktyg och en osäker omvärld där digital information riskerar att förloras, spridas eller förvanskas gör frågan viktigare än någonsin tidigare.

Kommuners digitala informationshantering styrs enligt lagkrav och det är viktigt med enkla, tydliga regler som gör det lätt att göra rätt bedömning vid lagring och delning av den digitala informationen.

Hur vi hanterar digital information är en viktig del av ett strukturerat informationssäkerhetsarbete, men det finns även andra viktiga delar.

För att få mer information kring informationssäkerhet bör du vara väl insatt i de styrdokument, utbildningar och regler som gäller i Bengtsfors, Färgelanda och Åmål. Mer information kan du få via ditt intranät eller via din närmaste chef.

För riktlinjer kring användning av artificiell intelligens (AI) så finns ett separat regelverk för detta.

Innehåll

Förenklad sammanfattning i korthet.....	4
Lagra	5
Molnlagring	5
Verksamhetssystem	5
Lokal serverlagring (exempelvis G-mapp, H-mapp osv.)	6
Kunskapsbanken (Infocaption).....	6
Lagring på extern disk (hårddisk, USB-minne)	7
Lokal lagring på den egna datorn (C:)	7
Säkerhetsskyddsklassificerade uppgifter	7
Dela och överföra	8
Delade filer via molnet (Onedrive och/eller Teams/Sharepoint)	8
Delade mappar på lokal server.....	9
Teamssamtal och videomöten.....	9
Telefonsamtal	10
SMS	10
Säkra videomöten.....	10
I verksamhetssystem.....	10
E-post (Outlook).....	11
Digital post (Kivra, Min Myndighetspost m.fl.)	11
Säkra meddelanden	11
Säker Digital Kommunikation (SDK)	11
Signalskyddssystem	12
Val av kanal ur ett invånarperspektiv.....	12
Medarbetarperspektivet	13
Bilaga 1: Matrisbild över lagrings- och spridningsvägar	15
Bilaga 2: Praktisk exempelguide för att avgöra känslighetsnivå på information och personuppgifter	22

Förenklad sammanfattning i korthet

LAGRA

Molnlagring (Onedrive, Teams, Sharepoint)

Inga personuppgifter utöver enstaka och med mycket låg känslighet (exempelvis namn eller telefonnummer till kollegor) ingen känslig information.

I verksamhetssystem (Lifecare, Schoolsoft, Ecos, Ciceron m.fl.)

Ska vara förstahandsval för personuppgifter, känslig information/sekretess.

EJ säkerhetsskyddsklassad information.

Lokal serverlagring (G:, H: V: etc.)

Personuppgifter, känslig information/sekretess, om det saknas verksamhetssystem. EJ säkerhetsskyddsklassad information. Var noga med VEM som har tillgång till mappen. Endast de som MÅSTE ha information, ska ha tillgång.

DELA INFORMATION

Delade filer via molnet (Onedrive, Teams, Sharepoint), samt Teams-chatt

Inga personuppgifter, ingen känslig information

E-post

Inga personuppgifter, ingen känslig information

Säkra meddelanden, Säker Digital Kommunikation.

Ska vara förstahandsval för personuppgifter, känslig information/sekretess. EJ säkerhetsskyddsklassad information.

Teamsmöten/Teamssamtal/Telefonsamtal

Godkänt för personuppgifter och information som har viss känslighet, förutsatt att användaren vet hur ett säkert samtal/möte ska arrangeras.

Säkra videomöten

Godkänt för känsliga personuppgifter och känslig information, förutsatt att användaren vet hur ett säkert samtal/möte ska arrangeras.

Signalskyddssystem

Används för att skydda säkerhetsskyddsklassificerade uppgifter när dessa ska kommuniceras. Kontakta Säkerhetschef eller säkerhetsskyddschef om behov uppstår.

Lagra

Hur information ska lagras beror på vilken typ av information det handlar om.

Generellt finns det följande lagringsalternativ:

Molnlagring (Onedrive, Teams, Sharepoint)

Här ska personliga dokument lagras (Onedrive) samt information som behöver delas med kollegor (Onedrive, Teams eller Sharepoint). Men endast information som är fri från personuppgifter som har någon form av känslighet och som inte är sekretessbelagd.¹

Exempel på sådan information kan vara arbetsmaterial som tjänsteskrivelser eller utredningar, planeringsdokument, minnesanteckningar, arbetsrutiner för din arbetsgrupp (teams) och annat.

Molnlagring är ett flexibelt och smidigt sätt att lagra information för snabb och enkel åtkomst, exempelvis från flera olika typer av enheter. Men det bedöms inte vara en säker plats för känslig information, därför är det inte tillåtet att lagra sådan information här. Säkerhetsbedömningen av molnlagring grundas sig i juridiska och regulatoriska faktorer, inte IT-tekniska.

Skillnader på olika former av molnlagring:

Onedrive – Din personliga molnlagring. Den är kopplad till dig som användare och som standard är inte informationen åtkomlig för någon annan i organisationen. Enstaka filer eller mappar kan delas med kollegor som bjuds in genom "delning". När du går i pension eller avslutar din anställning, försvinner allt i din Onedrive 90 dagar efter att du slutat.

Teams/Sharepoint – Denna molnlagring är primärt byggd för att du ska lagra och dela information ihop med andra. Det kan vara din arbetsgrupp eller hela organisationen. När ett team skapas, lagras själva filerna i Sharepoint, vilket få användare inser eller behöver veta. Men Sharepoint används också ofta som intranät eller som en molnbaserad mappstruktur där exempelvis styrande dokument, blanketter, nyheter och annan information förvaras som ska delas av hela kommunen, eller lite större men avgränsade delar av den, som en förvaltning eller ett arbetsställe.

Verksamhetssystem (exempelvis Lifecare, Schoolsoft, Nova, Ciceron m.fl.).

Det verksamhetssystem som medarbetaren fått tillgång till är inköpt och designat

¹ Det är nästan omöjligt att spara digital information utan någon form av personuppgifter, exempelvis författarens namn, kontaktuppgifter, eller uppgifter som går att härleda till andra tjänstepersoner etcetera. Denna typ av personuppgifter kan betecknas som okänsliga. Uppgifter om brukare, kommuninvånare, elever eller sammanställningar av större mängder personuppgifter är dock exempel på personuppgifter som inte får förekomma i molntjänster.

för att uppfylla alla säkerhetskrav som krävs för att hantera de ärenden och den information som det är avsett för. Detta är en mycket säker form av lagring och här ska så mycket som möjligt av kommunernas information lagras. Det är viktigt att medarbetaren får korrekt och uppdaterad information om HUR hen ska arbeta i systemet.

Lokal serverlagring (exempelvis G-mapp, H-mapp osv.)

Lokal serverlagring innebär att information lagras på servrar som endast Bengtsfors, Färgelanda och Åmål har tillgång till och som står, rent fysiskt, i de samverkande kommunernas lokaler. Informationen säkerhetskopieras även lokalt. Ingen extern part har normalt IT-teknisk, fysisk eller juridisk/regulatorisk åtkomst till servrar eller information.

För medarbetare i Bengtsfors, Färgelanda och Åmål finns det två typer av lokal lagring. Det ena är en personlig mapp på servern. Denna mapp har bara den enskilde medarbetaren åtkomst till. Här ska endast lagras information med personuppgifter/sekretess om det inte finns något verksamhetssystem att lägga in dessa i. Den personliga mappen tas bort när anställningen avslutas, så det är viktigt att komma ihåg att överföra information av värde till annan lagringsyta.

Den andra typen av lokal lagring är en gemensam mapp som – om det inte redan finns en sådan mapp för enheten – kan beställas från IT- och digitaliseringsenheten via IT-portalen. Till denna mapp kan en hel enhet ha tillgång, eller andra personer i den egna kommuner, utifrån vad beställaren önskar. Det är viktigt att komma ihåg vilka som givits tillgång till mappen och uppdatera när någons behörighet ska läggas till eller tas bort, för att säkerställa att endast de som behöver ta del av informationen, har tillgång till den.

Kunskapsbanken (Infocaption)

Kunskapsbanken är inte avsett som en lagringsplats för information.

Kunskapsbanken är en pedagogisk plattform för att utbilda och sprida kunskap. Exempelvis kompetenshöjande material där hela enheter, yrkesgrupper eller organisationer ska få den kunskap som krävs för att leva upp till riktlinjer/lagar, eller för att utveckla eller behålla gemensamma arbetssätt.

Andra lagringssätt samt undantag:

Lagring på extern disk (hårddisk, USB-minne)

Denna form av lagring bör endast användas i undantagsfall, eftersom informationen löper ökad risk att spridas på ett sätt som inte varit avsett. Det kan vara nödvändigt att använda extern lagring för att exempelvis överföra sekretessinformation eller information med känsliga personuppgifter i samband med att en medarbetare slutar sin anställning, för att säkerställa att information inte försvinner. Det är då viktigt att på ett korrekt sätt radera informationen när överföringen är avslutad. Om du är osäker på hur du ska radera information på ett säkert sätt, kontakta IT- och digitaliseringsenheten.

När lagring på externa diskar ska ske, får du endast använda utrustning som du fått från IT- och digitaliseringsenheten i Bengtsfors, Färgelanda och Åmål. Det är endast tillåtet att använda denna utrustning i maskiner som kommer från arbetsgivaren. Det är alltså INTE tillåtet att använda privat införskaffade USB-minnen eller hårddiskar, eller att ansluta en extern disk från IT- och digitaliseringsenheten till en privat dator.

Lokal lagring på den egna datorn (C:)

Denna form av lagring är inte tillåten för någon form av information, annat än i sällsynta undantagsfall. Det främsta skälet till detta är att det kan vara svårt att veta om informationen speglas upp i molntjänster (Onedrive) via synkroniserade mappar, samt att informationen blir extremt sårbar för tekniska problem. Om datorn försvinner eller går sönder är all information borta och går sannolikt inte att återskapa.

Säkerhetsskyddsklassificerade uppgifter

Vissa uppdrag i kommunen innebär att medarbetaren kan komma i kontakt med information som är "säkerhetsskyddsklassad" (säkerhetsskyddsklassificerade uppgifter). Med säkerhetsskyddsklassificerade uppgifter avses information som rör verksamhet av betydelse för Sveriges säkerhet och som därför omfattas av sekretess. Endast den som är behörig och har genomgått godkänd säkerhetsprövning får komma i kontakt med sådana uppgifter. Denna typ av information får inte hanteras i vår vanliga IT-miljö. I Riktlinjer för säkerhetsskydd med anslutande anvisningar från säkerhetsskyddschefen beskrivs hur kommunen ska arbeta med säkerhetsskyddsklassificerade uppgifter. För stöd att hantera den här typen av uppgifter kontakta kommunens säkerhetsskyddschef.

Dela och överföra

Det finns ofta behov av att dela eller sprida den information som en medarbetare i Bengtsfors, Färgelanda och Åmål framställt eller lagrat.

På samma sätt som vid val av lagring, faller det på den enskilde medarbetaren göra en bedömning av känslighetsgraden i materialet. För att kunna göra denna bedömning krävs en grundläggande utbildning i informationssäkerhet och klassning av dokument. Information om detta finns på respektive kommuns intranät och du kan också kontakta din närmaste chef om du känner dig osäker.

De sätt att sprida information som medarbetaren har att välja på är:

Delade filer via molnet (Onedrive och/eller Teams/Sharepoint)

Det kan ofta krävas att flera kollegor arbetar i samma dokument. Då kan ett delat dokument på Onedrive eller filer i ett delat Team vara ett bra alternativ. Det går att styra vilka som ska ha tillgång till olika dokument eller mappar. Det går också att styra vilka rättigheter den som dokumentet delas med ska ha. Ska de bara kunna läsa? Eller också redigera? Att dela filer är ett sätt att dela information som passar intern delning av information som inte innehåller känsligare personuppgifter eller omfattas av sekretess.

Eftersom Onedrive är en personlig molnlagring så är delning av filer här främst lämpligt om det rör en arbetsuppgift där medarbetaren är relativt självständig, men exempelvis vill att en kollega ska läsa igenom och lämna synpunkter.

Att dela filer via Teams/Sharepoint är lämpligare om information ska delas med en lite större arbetsgrupp. Det är också en bättre teknik om informationen som delas inte är personligt arbetsmaterial utan ska tillhöra och förvaltas av exempelvis en grupp medarbetare, som exempelvis en enhet. Eftersom denna lagring inte är personlig så säkerställs att materialet finns kvar och är tillgängligt även när en medarbetare slutar.

I Teams finns även chatmöjligheten och detta sätt att sprida information eller kommunicera är det sätt som rekommenderas för vardaglig, intern kommunikation. Tänk på att samma begränsningar gäller för chattar som för lagring av filer: du får inte kommunicera personuppgifter eller kommunicera information som omfattas av sekretess.

Delade mappar på lokal server

De delade mappar som beskrivits under rubriken "Lagra" är en form av delning som är säker, utifrån personuppgifter och sekretess. Däremot bygger informationssäkerhet och försiktighet med personuppgifter på att ENDAST medarbetare som behöver informationen, ska ta del av den. Att lägga information som omfattas av sekretess eller samling av personuppgifter i en mapp som är tillgänglig för en hel enhet, innebär ofta att fler än nödvändigt får tillgång. I dessa fall behöver ansvarig chef beställa separata undermappar i enhetens mappstruktur och noga styra/uppdatera vilka medarbetare som ska ha tillgång.

Teamssamtal och videomöten

Teams erbjuder också möjlighet för ljudsamtal och videomöten. Samma bedömning av säkerheten gäller för dessa kommunikationskanaler, men det är möjligt att kommunicera personuppgifter eller information av viss känslighet via samtal/videomöten, under vissa omständigheter. Dessa omständigheter hänger samman med handhavande och är:

- Spelas mötet in eller transkriberas? Då är det INTE tillåtet att kommunicera personuppgifter eller känslig information.
- Har mötet symbolen för krypterad anslutning synlig (hänglås)? I så fall är kommunikationen säker nog att kommunicera personuppgifter eller information av viss känslighet.
- Använder samtliga mötesdeltagare headset/hörlurar och sitter på ett sådant sätt (i stängt rum där endast samtalsdeltagarna finns) att muntlig information inte riskerar att överhöras? Då kan personuppgifter eller information av viss känslighet kommuniceras.
- Är alla mötesdeltagare säkra på identiteten hos övriga deltagare? I många fall känner kollegor igen varandra eller invånare från tidigare kontakter, på röst och utseende. Om tveksamhet finns kring identitet ska mötesdeltagare identifiera sig genom att tydligt visa upp en giltig identitetshandling och kameror ska vara påslagna.
- I teamssamtal eller teamsmöten får inte kommunikation ske kring särskilt känsliga personuppgifter eller information där sekretesskyddet är starkt, liksom information som bedömts vara säkerhetskyddsklassad och därmed exempelvis kan påverka rikets säkerhet.
- Tänk på att videomöten ofta har möteschatt. Detta är inte en lämplig plats att skriva ut känsligare typer av personuppgifter eller information.

Telefonsamtal

Telefonsamtal bedöms vara något säkrare än teamssamtal, genom att det använder sig av telefonnätet som är mer osannolikt att bli utsatt för intrång eller avlyssning. Du bör dock iaktta samma försiktighet kring eventuell överhörning och identitet hos samtalspartnern som vid teamssamtal.

SMS

Ett SMS kan användas för att kommunicera påminnelse, exempelvis att lämna tillbaka böcker till bibliotek, påminnelse inför bokat möte eller för att snabbt och brett kommunicera störningar i service, som gata eller vatten/avlopp. Det har bred träffyta och kan via olika tjänsteverktyg som kommunens kommunikatör handhar, nå ut till alla kommuninvånare med mobiltelefon. I SMS ska inte information som omfattas av sekretess eller en enskild invånares personuppgifter spridas.

Säkra videomöten

Bengtsfors, Färgelanda och Åmål har en teknologi för Säkra videomöten. Dessa videomöten är säkerhetsförstärkta och har identitetskontroll för den som deltar i mötena, via e-legitimation. Detta sätt att kommunicera är därmed säkert och rekommenderas för kommunikation av känsliga personuppgifter och information som omfattas av sekretess. Precis som vid vanliga videomöten, tänk på att möteschat är olämpligt att skriva ut känsliga personuppgifter eller information som omfattas av sekretess.

I verksamhetssystem

I många verksamhetssystem går det att ge behörighet till ärenden eller enskilda handlingar till kollegor och i vissa fall även till invånare/brukare. Detta sätt att sprida information är ett säkert och tillförlitligt sätt att dela information, men hur det görs och i vilka situationer det ska göras, skiljer sig åt mellan de olika systemen och verksamheter. Medarbetaren bör kontakta närmaste chef eller systemets systemförvaltare för mer information och kunskap, om osäkerhet råder.

För exempelvis barnomsorg eller utbildning är verksamhetssystemet det primära sättet att ha kontakt med elever och vårdnadshavare i frågor som rör verksamhetsinnehållet. Normalt är inte ett verksamhetssystem en väg som ska användas för information som är av karaktären "mycket viktig information" eller myndighetsbeslut. För denna form av kommunikation är andra kanaler, främst digital post, ett bättre alternativ.

E-post (Outlook)

Med E-post kommunicerar medarbetaren i okänsliga frågor, utan personuppgifter, både externt och internt.² Mellan kollegor i vardaglig, arbetsrelaterad kommunikation, ska Teams-chattar användas av effektivitetsskäl samt för att inte riskera att försena korrespondens med invånare eller externa parter som är högt prioriterade.

Digital post (Kivra, Min Myndighetspost m.fl.)

Den digitala posten är ett säkert, miljövänligt och kostnadseffektivt alternativ till papperspost. Digital post ska vara förstahandsalternativet för att skicka ut information av viss/högre dignitet, som exempelvis viktig information för individen, så som ett myndighetsbeslut. När man skickar ett meddelande med Digital post, görs en slagning mot ett nationellt register för digitala myndighetsbrevlådor. Om den individ som kommunen vill kommunicera med har anmält en digital brevlåda, kommer meddelandet att skickas dit. Om invånaren saknar digital brevlåda, kommer meddelanden att automatiskt skrivas ut, kuverteras och skickas till invånaren med traditionell papperspost.

Säkra meddelanden

Säkra meddelanden är en säker, krypterad form av elektronisk post där både avsändaren och mottagaren behöver legitimera sig med digital legitimation, exempelvis Bank-ID. Detta är det sätt som du ska dela information som innehåller personuppgifter samt känslig information som eventuellt är sekretessklassad. Säkra meddelanden kan användas både för att skicka information inom kommunen och till externa parter, som externa konsulter, kontakter på andra myndigheter eller privatpersoner.

Säker Digital Kommunikation (SDK)

Säker Digital Kommunikation är en nationell standard för digital kommunikation mellan myndigheter. Liksom säkra meddelanden så krävs digital legitimation för att skicka och ta emot kommunikationen.

Skillnaden mellan Säkra Meddelanden och Säker Digital kommunikation är att Säkra meddelanden skickas mellan individer. Säker Digital Kommunikation sker mellan myndigheter. Det innebär att om exempelvis sjukvården, Polisen eller

² Precis som i fallet med molnlagring så ska begreppet "personuppgifter" tolkas som att de vardagliga personuppgifter som krävs för att kommunicera, är acceptabla. Exempelvis namn och kontaktuppgifter på tjänsteperson etcetera.

Försäkringskassan vill kommunicera med Bengtsfors-, Färgelanda- eller Åmåls kommun, så kommer de att skicka sitt beslut eller information via Säker Digital Kommunikation, om den innehåller känsliga personuppgifter eller sekretessinformation.

Meddelandet skickas till en myndighetsbrevlåda i SDK som inte är personlig, utan som bevakas av tilldelade handläggare och därefter hanteras inom myndigheten/kommunen. En dom från en domstol gentemot en kommuns myndighetsutövning är exempel på sådan kommunikation, liksom en begäran om information från exempelvis kommunens skolverksamhet eller socialtjänst, från psykiatrimottagningar eller polismyndigheten.

Säker Digital Kommunikation är en säkrare väg att skicka känslig information i jämförelse med Säkra meddelanden, just eftersom informationen når en annan myndighet som helhet. Även om en viss handläggare är otillgänglig eller om det saknas personliga kontaktvägar i berörd myndighet, kommer kommunikationen att nå fram och tas omhand av den mottagande myndigheten.

Signalskyddssystem

För att kommunicera säkerhetsklassificerade uppgifter ska ett signalskyddssystem användas, t.ex. Signe.

Exempel på sådan information kan vara säkerhetskyddsklassad information från Länsstyrelsen eller Försvarmakten som – om den hanteras orätt eller sprids oavsiktligt – skulle kunna orsaka skada rörande rikets säkerhet.

Säkerhetsklassad information enligt säkerhetsskyddslagen som behöver kommuniceras med stöd av signalskyddssystem utförs alltid av säkerhetsskyddschef eller annan behörig inom signalskyddsorganisationen.

Val av kanal ur ett invånarperspektiv

När det gäller att dela information från någon av de samverkande kommunerna så finns det överväganden som inte strikt rör informationssäkerhet, IT-säkerhet eller personuppgiftshantering.

Det är viktigt att respektive verksamhet gör samlade, konsekventa kanalval bland de tillgängliga kanalerna för olika typer av kommunikation och håller fast vid dessa. Annars finns risken att kommuninvånaren blir förvirrad, att förtroendet för

den avsändande kommunen undergrävs och att information inte når fram till invånaren.

Valet av kanal bör utgå från var invånaren finner det naturligt och logiskt att finna information i sin kontakt med myndigheter, främst med utgångspunkt i vilken tyngd och frekvens informationen har. Generellt bör följande tillämpningar betraktas som vedertagna principer för myndigheters sätt att kommunicera digitalt:

- **Kommunicering i löpande kontakter mellan myndighet/kommun och invånare** sker via ett verksamhetssystem eller en eventuell inloggningsbar invånarapp/E-tjänsteportal. Detta gäller exempelvis frågor där invånaren är väl medveten om att ett informationsutbyte är etablerat, exempelvis genom ett serviceförhållande eller att ett ärende är väckt. Exempel på detta är att man har ett barn i förskola/skola, och att information utbyts kring denna service. Avisering av friluftsdagar, ändringar i rutiner på skolan mm. Finns inget verksamhetssystem så kan E-post vara ett bra alternativ, så länge inte personuppgifter eller sekretessinformation blandas in.
- **Kommunicering av myndighetsbeslut** har tyngre dignitet och förväntas därför gå via andra kanaler. Det kan handla om att bevilja eller avslå en begäran från invånaren, eller att myndigheten har kommit fram till att besluta om en åtgärd som på något sätt påverkar invånarens liv. Det kan röra sig om placeringar inom skola/omsorg, bygglovsärenden med mera. För denna typ av kommunikation bör varken e-post eller verksamhetssystem användas. Digital post bör vara ett naturligt alternativ, men varje verksamhet behöver ta ställning till om innehållet kan kommuniceras denna väg. Ofta går det bra, men det kan i vissa fall vara fråga om mycket känslig information där rekommenderad post eller delgivning kan krävas.

Om den del av kommunen där du arbetar inte har tagit fram enkla och tydliga regler för vilken typ av kommunikation som ni ska skicka till kommuninvånaren i respektive kanal, ta upp frågan med din närmaste chef.

Medarbetarperspektivet

På samma sätt som invånaren, har medarbetare i offentlig förvaltning en förväntan av konsekvent delning av information/kommunikation. Olika kanaler associeras med olika graderingar av viktig information och det är viktigt att verksamheter har en gemensam bild av var och hur man kommunicerar internt.

Som nämnts tidigare bör Teams-chattar vara det primära valet för vardaglig arbetskommunikation mellan kollegor. Detta eftersom E-post kan innehålla kommunikation från externa, viktiga parter som invånare, myndigheter eller media. För dessa förfrågningar måste förvaltningen kunna respondera på snabbt, enligt myndigheters serviceskyldighet.

Därför är det olämpligt att fylla e-postkorgar med interna arbetskonversationer som riskerar att fördröja svar på viktiga externa förfrågningar, eller kritisk intern kommunikation.

E-post, tillsammans med information via intranät och muntlig kommunikation vid veckomöten/arbetsplatsträffar bör vara det primära valet för viktig organisationsinformation.

För all intern kommunikation som innehåller personuppgifter och information som omfattas av sekretess ska Säkra meddelanden användas.

Om denna grundprincip tillämpas konsekvent, ökar kommunernas förmåga att dela information effektivt.

Bilaga 1: Matrisbild över lagrings- och spridningsvägar

	Lämpligt för:	Olämpligt för:	Får jag använda för personuppgifter?	Får jag använda för sekretess?
Lagra				
Molnlagring (Onedrive, Teams, Sharepoint)	Personligt arbetsmaterial som INTE innehåller personuppgifter eller omfattas av sekretess. Material som ska delas med ett begränsat antal kollegor inom organisationen. Sådant som du vill ha enkel tillgång till från olika typer av tekniska enheter och platser.	Personuppgifter information som omfattas av sekretess. Material som ska nå ut brett i organisationen.	NEJ	NEJ
Verksamhetssystem	Allt som rör verksamheten. Sekretessbelagd information och personuppgifter även av känslig art.	Material som du vill kunna dela brett i organisationen. Dokument som beskriver HUR verksamheten ska arbeta, exempelvis rutiner och sådant som många behöver ha snabb och flexibel åtkomst till.	JA	JA
Lokal serverlagring (G, H)	Personligt arbetsmaterial som innehåller personuppgifter eller information som omfattas av sekretess.	Information som ska spridas till större målgrupper. Material som ska vara åtkomligt från olika typer av tekniska enheter eller från olika platser på ett smidigt sätt.	JA , men du måste vara säker på att platsen du lagrar på endast är tillgänglig för den som behöver informationen	JA , men du måste vara säker på att platsen du lagrar på endast är tillgänglig för den som behöver informationen

Kunskapsbanken (Infocaption)	Utbildningsmaterial , kompetensutveckling. Material som ska ge ny eller fördjupad kunskap kring fakta eller arbetssätt.	Styrdokument. Kunskapsbanken är inte en lagringsplats för detta, utan ska utbilda. Personuppgifter och sekretessbelagd information ska ej förekomma här.	Nej	Nej
Lagring på extern disk	Temporär information som i undantagsfall behöver flyttas från en lagringsplats till en annan och det saknas någon annan form av möjlig överföring.	Det mesta. Ska användas endast i undantagsfall och efter att andra möjligheter utretts.	JA , men denna lagringsform har flera risker och ska endast användas i undantagsfall. Du behöver nog säkerställa förvaring och hantering för att lagringen ska vara säker.	JA , men denna lagringsform har flera risker och ska endast användas i undantagsfall. Du behöver nog säkerställa förvaring och hantering för att lagringen ska vara säker.
Lagring på lokal dator	Ingenting	Allt	NEJ , du ska aldrig spara information lokalt på din dator.	NEJ , du ska aldrig spara information lokalt på din dator.
Dela och överföra				
Delade filer i molnet (Onedrive, Teams, Sharepoint)	Okänsligt material utan personuppgifter som flera kollegor ska samarbeta kring.	Ditt personliga arbetsmaterial, information som innehåller annat än okänsliga personuppgifter och sekretessinformation.	NEJ	NEJ

Teamssamtal och videomöten	Möten och samtal där endast mindre känsliga personuppgifter eller information förekommer och som har glädje av olika typer av tekniska funktioner som transkriberingar, delning av bilder/skärmar. Passar bra för två eller fler deltagare.	Möten och samtal för känsliga personuppgifter.	JA , du får dela personuppgifter och information som har en viss grad av känslighet, förutsatt att du säkerställt att du uppfyllt kriterierna för att samtalet/mötet ska vara säkert. För extra känsliga personuppgifter eller information av högre känslighet är inte detta rätt sätt att sprida/dela.	JA , du får dela personuppgifter och information som har en viss grad av känslighet, förutsatt att du säkerställt att du uppfyllt kriterierna för att samtalet/mötet ska vara säkert. För extra känsliga personuppgifter eller information av högre känslighet är inte detta rätt sätt att sprida/dela.
SMS	Viktig, bred information till invånare kring driftstörningar eller nödsituationer. Påminnelser om exempelvis bokade möten, bibliotekslån eller liknande.	All annan information.	Nej	Nej

Telefonsamtal	Samtal/möten mellan två personer, där en något högre grad av känsliga personuppgifter eller information som omfattas av sekretess kan förekomma och där inte avancerade tekniska funktioner som transkriberingar, delning av bilder/skärmar är nödvändigt.	Möten och samtal för känsliga personuppgifter.	JA , du får dela personuppgifter och information som har en viss grad av känslighet, förutsatt att du säkerställt att du uppfyllt kriterierna för att samtalet/mötet ska vara säkert. För extra känsliga personuppgifter eller information av högre känslighet är inte detta rätt sätt att sprida/dela.	JA , du får dela personuppgifter och information som har en viss grad av känslighet, förutsatt att du säkerställt att du uppfyllt kriterierna för att samtalet/mötet ska vara säkert. För extra känsliga personuppgifter eller information av högre känslighet är inte detta rätt sätt att sprida/dela.
Säkra videomöten	Samtal/möten mellan två eller fler personer där känsliga personuppgifter eller information som omgärdas av stark sekretess.	Samtal/möten mellan två eller flera personer där inte känsliga personuppgifter eller känslig information delas, samtal och möten där mötesdeltagare vill ha tillgång till avancerade tekniska funktioner som transkriberingar, inspelning, delade skärmar med mera.	JA	JA

Via verksamhetssystem	Kommunikation mellan kollegor eller mellan medarbetare och invånare i frågor där känsliga personuppgifter och sekretessbelagd information förekommer.	Samarbete där inte alla deltagare har tillgång till verksamhetssystem eller all info i detsamma, arbete på koncept eller arbetsstadiet. I verksamhetssystem lagras skarp information och färdigställda handlingar, journaler och elevakter. Det är inte en lämplig arena för experimentellt arbete. För sådan aktivitet erbjuder de flesta leverantörer "testmiljöer", tomma på skarp information.	JA	JA
E-post (Outlook)	Vardaglig och okänslig kommunikation med externa parter, eller med kollegor som du inte har en Teams-yta tillsammans med. Teamschattar bör vara ditt första alternativ för vardaglig kommunikation med kollegor. Ett e-postutskick kan också vara ett bra sätt att sprida viktig information som behöver nå ut inom din organisation eller kommun.	Kommunikation som innehåller annat än okänsliga personuppgifter eller sekretessbelagd information. Återkommande kommunikation med kollegor inom organisationen.	NEJ	NEJ

Digital post	Kommunikation mellan kommunen och invånaren för att informera om viktigare förändringar i exempelvis service, myndighetsbeslut och annan viktig information som kan innehålla personuppgifter och information som kan vara sekretessbelagd.	Tvåvägskommunikation eller dialog. Mindre viktig information - invånaren har en förväntan att information som skickas i papperspost eller till en elektronisk brevlåda är av en viss dignitet.	JA, du får dela personuppgifter och information som har en viss grad av känslighet. Det är dock viktigt att din verksamhet har gjort bedömningen kring vilka informationstyper som är godkänd att skicka som digital post.	JA, du får dela personuppgifter och information som har en viss grad av känslighet. Det är dock viktigt att din verksamhet har gjort bedömningen kring vilka informationstyper som är godkänd att skicka som digital post.
Säkra meddelanden	För att dela information med en kollega som innehåller känsliga personuppgifter eller sekretessbelagd information passar Säkra meddelanden bra.	Information av lägre vikt, marknadsföring eller breda utskick är inte lämpligt att skicka via denna kanal.	JA	JA
Säker Digital Kommunikation (SDK)	SDK är den metod du ska använda för att kommunicera säkert med andra myndigheter. Här kan känsliga personuppgifter och sekretessbelagd information skickas och denna väg att dela information kommer tryggt fram, eftersom mottagande organisation tar ett samlat ansvar för att dagligen kontrollera brevlådan, till skillnad från Säkra meddelanden som är personberoende.	Information av lägre vikt, marknadsföring eller breda utskick är inte lämpligt att skicka via denna kanal.	JA	JA

Signalskyddssystem	Med signalskyddssystem kan din signalskyddsorganisation hjälpa dig att skicka säkerhetsklassad information till andra myndigheter kring exempelvis försvarsförmåga, information om skyddsobjekt eller kritisk infrastruktur.	All annan information än den säkerhetsklassade informationen ska väljas andra kanaler.	JA	JA
Specialfall:				
Säkerhetskyddsklassificerad information (begränsat hemlig)	Endast den som är behörig och har genomgått godkänd säkerhetsprövning får hantera säkerhetskyddsklassificerade uppgifter. Uppgifterna får inte hanteras i ordinarie it-miljö utan enligt riktlinjer för säkerhetsskydd med anvisningar. Kontakta säkerhetsskyddschef innan du tar emot, lagrar, sprider eller på annat sätt hanterar säkerhetsklassad information.			

Bilaga 2: Praktisk exempelguide för att avgöra känslighetsnivå på information och personuppgifter

OBS: Denna bilaga har som mål att erbjuda praktisk guidning till hur kommunens medarbetare ska hantera och bedöma informations känslighet. Den gör inte anspråk på att i detalj återge termer eller bedömningar som regleras i exempelvis dataskyddsförordningen eller cybersäkerhetslagen. För djupgående analyser eller särskilt känsliga fall bör relevant lagstiftning alltid studeras.

Personuppgifter/öppen information

Personuppgifter och information som kan delas fritt, skickas via e-post och delas på Teams.

Tänk på att personuppgifter alltid ska hanteras restriktivt, så undvik att spara personuppgifter på fler ställen än nödvändigt eller att spara sådant som du inte längre har behov av.

Exempel:

Namn	Registreringsnummer
Födelsedatum	Fastighetsbeteckning
Adress	Annan information som inte regleras av OSL
Telefonnummer	

Särskilt skyddsvärda personuppgifter/skyddsvärd information

Särskilt skyddsvärda personuppgifter och information ska delas restriktivt både internt och externt. Använd inte Teams eller Outlook för att spara eller dela sådana uppgifter. Denna information kan delas via Säkra meddelanden, SDK och i säkra videosamtal, samt sparas i avsett verksamhetssystem eller i lokal servermapp.

Exempel:

Löneuppgifter	Systembeskrivningar
Fullständiga personnummer	Konsekvensbedömningar
Fullständiga personallistor	Systemanalyser
Uppgifter från utvecklingssamtal	Vissa typer av detaljerade kartor
Skyddade personuppgifter	

Känsliga personuppgifter/sekretessbelagd information

Känsliga personuppgifter och sekretessbelagd information ska helst inte delas alls utanför myndigheten och restriktivt inom den. Outlook och andra mailprogram samt Teams ska aldrig användas för att spara eller dela dessa uppgifter. Denna information kan delas via Säkra meddelanden, SDK och i säkra videosamtal, samt sparas i avsett verksamhetssystem eller i lokal servermapp.

Det är viktigt att komma ihåg att en personuppgift kan vara känslig utifrån sammanhanget den förekommer i.

Exempel:

Religion	Kontinuitetsplanering
Etnicitet	Krisplaner
Politisk åskådning	Risk- och sårbarhetsanalyser
Sexuell läggning eller sexualliv	Underlag för säkerhetsprovning
Medlemskap i fackförening	Kryptonycklar
Hälsouppgifter	Vissa certifikat
Fingeravtryck	Vissa
Personuppgifter	

OBS! Enskilda bedömningar ska alltid göras när information och personuppgifter ska delas, både internt och externt.

