HEDEMORA KOMMUN	**STYRDOKUMENT**	Sida 1(6)
Skapad av: Säkerhetschefen	Datum 2021-11-22	Diarienummer: KS178-21 003
	Giltighet fr o m: 2022-05-17	Senast reviderad: -
Godkänt/antagen av: Kommunstyrelsen den 17 maj 2022 § 47		
Dokumentationsansvarig: Kommunsekreteraren		

Riktlinje för digital kommunikation

Dok. Kategori:	Riktlinjer
Stadie:	Beslutad
Gallring:	Bevaras
Kort beskrivning:	Riktlinje för hur anställda och förtroendevalda ska hantera digitala kommunikationsverktyg (e-post och andra digitala kommunikationsverktyg) i Hedemora kommuns förvaltningar och bolag

Hedemora kommuns olika styrdokument

Organiserade styrdokument Visar tydligt roll och ansvarsfördelning. - Reglemente - Delegationsordning - Bolagsordning	**Aktiverande styrdokument** Visar vad kommunen vill förändra och uppnå. - Strategi - Mål och budget - Program - Ägardirektiv - Handlingsplan och övrig plan - Förvaltningarnas verksamhetsplan - Bolagens affärsplan - Aktivitetsplan
Normerande styrdokument Tydliggör kommunens förhållningssätt och arbetssätt. - Policy - Riktlinje - Rutin och vägledning	**Regler för dem som bor och verkar i Hedemora kommun** Tydliggör villkoren för kommunal service och vilka krav kommunen ställer på de som bor och verkar i kommunen. - Avgifter (inkl. taxor) - Regler (inkl. lokala föreskrifter och lokala ordningar

Mer information om de olika styrdokumenten finns i Hedemora kommuns riktlinje ”Riktlinjer för styrdokument”.

Globala målen – Agenda 2030

Mål 16 i Agenda 2030 *handlar om Fredliga och inkluderande samhällen. Fredliga samhällen och frihet från våld utgör både ett mål och ett medel för hållbar utveckling. En väl fungerande statsförvaltning med ansvarsfulla institutioner, transparens och rättsstatens principer har alla ett fundamentalt egenvärde. De utgör grund för god samhällsstyrning inklusive korruptionsbekämpning och är viktiga drivkrafter för utveckling. Alla människor är lika inför lagen och ska ha lika tillgång till rättvisa samt ska ha möjlighet att utöva inflytande och ansvarsutkrävande över beslutsfattare. God samhällsstyrning och rättsstatens principer är grundläggande mål och medel för utveckling. Begreppen demokrati och de mänskliga rättigheterna återfinns inte uttryckligen under mål 16. Dessa begrepp förekommer dock tydligt i den politiska deklarationen i 2030-agendan.*

Delmål i mål 16

16.10 Säkerställa allmän tillgång till information och skydda grundläggande friheter, i enlighet med nationell lagstiftning och internationella avtal.

1. Inledning

1.1 Målgrupp och syfte

Målgrupp för denna riktlinje är medarbetare, chefer och förtroendevalda som använder sig av Hedemora kommuns digitala kommunikationsverktyg såsom e-postbrevlådor, det vill säga användare av myndighetsbrevlåda, funktionsbrevlåda eller individuell e-postbrevlåda, digitala mötesplattformar, digitala anslagstavlor, digitala kalendrar och digitala chattfunktioner m.m. Med kommunen nedan menas Hedemora kommuns nämnder (förvaltningar) och bolag.

Syftet med riktlinjen är att vara en samlad beskrivning av vad som gäller vid användning av digitala kommunikationsverktyg i alla kommunens verksamheter. Till denna riktlinje finns rutin som i detalj beskriver processer, ansvar och principer vid användning av olika digitala kommunikationsverktyg.

2. Riktlinje vid användning av e-post

2.1 Utgångspunkter vid användning av e-post

2.1.1 Offentlighetsprincipen och dataskyddsförordningen

Allmänhetens rätt att ta del av allmänna handlingar är skyddad i grundlag. E-post ska hanteras på motsvarande sätt som traditionella brev vad gäller offentlighet och sekretess, diarieföring, gallring och arkivering. Allmänhetens rätt till insyn få inte försämras när e-post används. Vid användning av e-post gäller alltid reglerna för registrering, tillhandahållande, gallring och arkivering av allmänna handlingar enligt offentlighetsprincipen. E-postmeddelande utan ärendeanknytning som skickats mellan tjänstepersoner inom en myndighet, dvs inom en förvaltning eller bolag, är inte en allmän handling.

E-postmeddelanden och bifogade filer ska bevaras och gallras i enlighet med dokumenthanteringsplan eller gallringsbeslut.

Enligt dataskyddsförordningen (EU 2016/679) är en e-post innehållande personuppgifter en personuppgiftsbehandling och det krävs därför en rättslig grund som tillåter att personuppgifterna behandlas i e-post. Beroende på ämne i e-posten kan den grunda sig på olika rättsliga grunder. Själva e-postadressen i sig är oftast en personuppgift och all annan information i meddelandet som kan kopplas till en enskild person är också personuppgifter. Den personuppgiftsbehandling som sker i e-post ska därför finnas med i organisationens förteckning över personuppgiftsbehandling och uppfylla alla andra krav i dataskyddsförordningen. E-post som inkommer till kommunens e-postbrevlådor och som innehåller extra skyddsvärda- och/eller känsliga personuppgifter eller annan integritetskänslig information (t ex sekretessbelagd information inkl. säkerhetskyddsklassificerad information) ska utan dröjsmål skiljas ut och hanteras i ärendehanteringssystem om det är ärenderelaterat eller på annan plats med tillräcklig säkerhet för sådana uppgifter.

Regelverk som styr e-posthanteringen återfinns bland annat i tryckfrihetsförordningen, offentlighets- och sekretesslagen, lagen om företagshemligheter, förvaltningslagen, dataskyddsförordningen, dataskyddslagen, nämnden/bolagets dokumenthanteringsplan, Hedemora kommuns arkivreglemente, riktlinje och rutin för e-post.

2.1.2 E-postsystemet är ett arbetsverktyg för kommunikation

E-postsystemet är ett arbetsverktyg för kommunikation och ska användas med gott omdöme. E-posten är inte något ”arkiv”, där information ska lagras.

2.1.3 Privat användning av e-post

Privat användning av e-post får endast ske i mycket begränsad omfattning och får inte

- inkräkta på ordinarie arbetsuppgifter,
- påverka kommunens IT-resurser i form av ökade kostnader eller innebära en ökad risk för spam eller
- i övrigt påverka lagringsutrymme och prestanda på ett negativt sätt.

Det ska tydligt framgå när e-post skickas privat och tjänstesignatur får aldrig användas när e-postmeddelanden skickas i privata ärenden.

2.2 Myndighetsbrevlåda och funktionsbrevlåda i förvaltningar och bolag

Alla nämnder (förvaltningar) och bolag i Hedemora kommun ska

- ha minst en officiell e-postadress (myndighetsbrevlåda) och ska kunna ta emot handlingar via e-post som kontrolleras minst en gång per arbetsdag,
- vid behov upprätta en funktionsbrevlåda (som likt myndighetsbrevlådan är personoberoende) till vilken flera personer har tillgång till för att hantera e-post för att uppfylla lagkrav, rutiner och tjänstegarantier (gällande tjänstegarantier, se personalhandbok). Innan en funktionsbrevlåda sätts upp ska det finnas en skriftlig rutin som beskriver hur lådan ska hanteras,
- säkerställa att inkommen e-post till förvaltning och bolag hanteras utan dröjsmål enligt rutiner och kommunens tjänstegarantier,
- för att undvika personberoenden och att information inte är tillgänglig i en verksamhet använda myndighets- och funktionsbrevlåda istället för individuell e-postbrevlåda.

2.3 Hantering av individuell e-postbrevlåda

Alla medarbetare, chefer och förtroendevalda med individuell e-postbrevlåda är ansvariga för att kontrollera sin e-post och löpande skilja ut och utan dröjsmål hantera allmänna handlingar och personuppgifter enligt gällande regelverk och kommunens tjänstegarantier.

E-postanvändare som inte ger fullmakt till någon annan i verksamheten att ha tillgång till individuell e-postbrevlåda eller inte omdirigerar sin e-post till myndighetsbrevlåda eller funktionsbrevlåda är själv ansvarig att kontrollera e-posten även vid semester, föräldraledighet, sjukskrivning eller annan frånvaro.

E-postanvändare bör på eget initiativ tömma individuell e-postbrevlåda när anställning eller uppdrag upphör såvida inte e-postmeddelanden och tillhörande bilagor kan betraktas som allmän handling och ska diarieföras och/eller arkiveras eller förmedlas vidare till närmaste chef.

Om det finns handlingar kvar i individuell e-postbrevlåda, när e-postanvändare lämnat eller slutat sin anställning eller uppdrag, är utgångspunkten att dessa handlingar är av tillfällig eller ringa betydelse. I och med att man lämnat eller slutat sin anställning upphör omgående möjligheten för medarbetaren/uppdragstagaren att kunna ta del av sin individuella e-postbrevlåda.

2.4 Tekniska lösningar och skydd för inloggningsuppgifter

Endast de tekniska lösningar som IT-avdelningen tillhandahåller får användas för e-post, mobil e-post, synkronisering av kalenderfunktion, chattfunktioner och motsvarande funktioner.

Om e-postanvändare använder öppna nät vid behandling av personuppgifter ska denne ansvara för att:

1) överföring av uppgifterna görs på ett sådant sätt att inte obehöriga kan ta del av dessa och
2) elektronisk åtkomst eller direkt åtkomst till uppgifterna föregås av stark autentisering.

E-postanvändare har ansvar för och ska skydda personliga lösenord och hjälpmedel för autentisering så att de inte kan bli tillgängliga för obehöriga. Lösenord är personliga och får inte delas med andra personer. Om e-postanvändare misstänker att någon annan känner till det egna lösenordet ska lösenordet omgående bytas ut. Lösenordet ska vara kvalificerat och följa kommunens rutiner för lösenord.

E-postanvändare är skyldiga att följa gällande styrdokument kring informationssäkerhet och dataskydd och genomgå de informationssäkerhets- och dataskyddsutbildningar som anvisas.

2.5 Extra skyddsvärda- och/eller känsliga personuppgifter och annan integritetskänslig information (t ex sekretessbelagd information inkl. säkerhetsskyddsklassificerad information.

Skyddade IT-system för kommunikation, ex vis Mina sidor och liknande, ska i första hand användas i kommunikationen med medborgare, företag, myndigheter och andra organisationer. Om sådan inte är tillgänglig får information med känsliga- och extra skyddsvärda personuppgifter och annan integritetskänslig information (sekretesskyddad information och säkerhetsskyddsklassificerad information) hanteras enligt nedan.

Det är tillåtet att skicka sekretesskyddad information och information innehållande särskilt skyddsvärda- och/eller känsliga personuppgifter med säker e-post (t ex TrustedDialog, som är godkänd av IT-avdelningen). Förutsättningen är att e-posten ska ha en end-to-end- kryptering och i övrigt uppnå de säkerhetskrav/nivåer enligt lag som gäller för sekretesskyddad information och särskilt skyddsvärda- och känsliga personuppgifter. För säkerhetsskyddsklassificerad information gäller särskilda instruktioner.

Vad som är känsliga personuppgifter och särskilt skyddsvärda personuppgifter framgår av dataskyddsförordningen (EU 2016/679) och dataskyddslagen. Exempel på integritetskänsliga personuppgifter är uppgifter som omfattas av sekretess, rör en persons personliga sfär eller som på annat sätt värderar en persons sociala, ekonomiska eller liknande förhållanden. Även säkerhetsskyddsklassificerad information är sekretessbelagd.

3. Andra digitala kommunikationsverktyg än e-post

3.1 Utgångspunkter vid användning av andra digitala kommunikationsverktyg än e-post

Vid användning och hantering av andra digitala kommunikationsverktyg såsom exempelvis olika digitala mötesplattformar för digitala möten och videokonferenser**,** digitala anslagstavlor, digitala kalendrar och digitala chattfunktioner med flera ska Rutin för digitala kommunikation följas.

Digitala möten och videokonferenser genomförs oftast via media som inte uppfyller kommunens krav vad avser konfidentialitet. Innan mötet måste deltagare därför genomföra en riskanalys och fastställa hur man under och efter mötet ska agera för att minimera risken för att konfidentiell information sprids.

Utgångspunkten är att endast harmlösa personuppgifter får hanteras i digitala kommunikationsverktyg. Dispens kan dock beviljas efter särskilt beslut i informationssäkerhets- och dataskyddsrådet, se Riktlinje för informationssäkerhet och dataskydd.