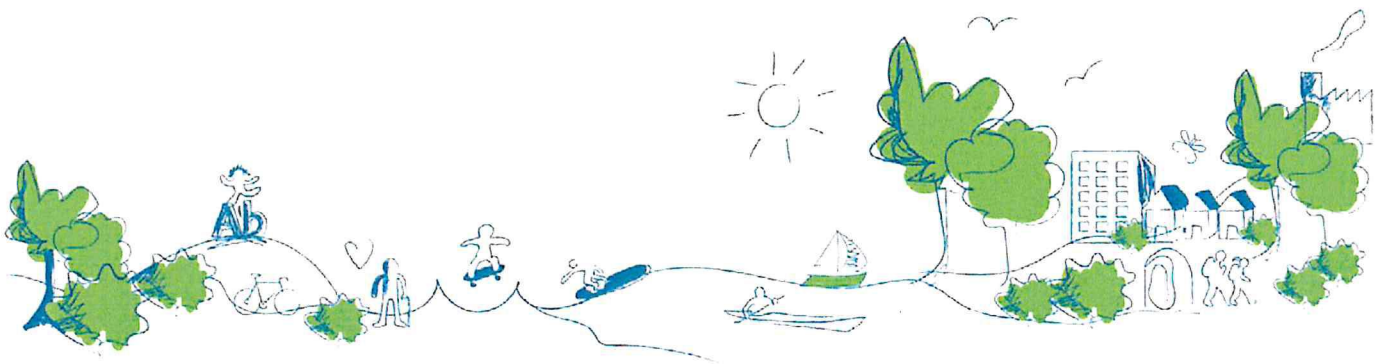
KS 2018/0210/005 - 10

Nynäshamns kommun

Revisionsdatum: 2018-08-08
Upprättad av: Per Österberg, IT- chef samt Yvonne Persson kommunjurist
Antagna av kommunfullmäktige den 2018-2018-09-19 § 140

Riktlinjer för användning av IT- och telefonistöd i Nynäshamns kommun



Innehåll

Inledning

Riktlinjerna gäller för anställda och förtroendevalda i Nynäshamns kommun och beskriver vilka förutsättningar som gäller för användning av IT-och telefonistöd. Med IT- och telefonistöd avses alla typer av installerade IT-lösningar eller molntjänster på datorer, läsplattor, telefoner och servrar. Detta gäller även om program eller funktioner kan uppfattas som gratis.

Ansvar och information

Syftet med dessa riktlinjer är att stödja användare inom kommunen i samband med användning av IT- och telefonistöd genom att beskriva och tydliggöra vilka regler och lagar som gäller samt hur man ska agera.

- Chef är ansvarig för att riktlinjerna görs kända bland sina medarbetare. Det är också chefs ansvar att vidta åtgärder om riktlinjerna inte efterföljs.
- Användare ansvarar för att följa dessa riktlinjer.

Användande

Utrustning som tillhandahålls av kommunen är arbetsredskap som anställda och förtroendevalda förfogar över för att kunna fullgöra sina arbetsuppgifter. Dock får man använda arbetsredskapen för privata icke kommersiella ändamål så länge detta inte inkräktar på dess funktioner.

Riktlinjer för arbete med Internet

Internet är ett effektivt och viktigt verktyg i arbetet. Möjligheterna att använda Internet innebär också ett ökat ansvar för anställda. Agera på Internet i enlighet med vår värdegrund så att det du förmedlar på nätet inte skadar varumärket.

Allmänt gäller att vid nedladdning av filer från Internet krävs att du har gott omdöme och endast hämtar in sådant som är relevant för arbetet och kommer från välrenommerade och säkra webbplatser. Ljud och videofilmer/filer som inte är relevanta till arbetet/verksamheten får inte laddas ned. Det är inte tillåtet att använda Nynäshamns kommuns utrustning och system för att olagligt "streama" musik eller filmer samt att ladda hem upphovsrättsskyddat material.

Sökning, nedladdning, överföring, distribution och innehav av kriminellt, rasistiskt, diskriminerande, pornografiskt eller material av våldskaraktär med hjälp av kommunens resurser är absolut förbjudet. Det är också absolut förbjudet att i otillbörliga syften söka kontakt alternativt stämma möte med andra människor och i synnerhet med barn via chatt, diskussionsgrupper eller andra forum.

Vid misstanke om missbruk finns möjlighet för arbetsgivaren att spåra användandet och vidta åtgärder.

Installation av utrustning och program

För att undvika problem med att olika program inte fungerar ihop, licenshantering m.m. ska alla datorprogram beställas hos servicedesk. Applikationer till smarta mobiler och läsplattor får laddas ner på egen bekostnad via tillverkarnas marknadsplatser. Dessa applikationer får inte användas för att ladda upp kommuninformation som dokument, register etc. i molntjänster.

Servicedesk har rätt att rensa den enskilde användarens IT- och telefonistöd från all information och alla program i den mån dessa riktlinjer inte har följts eller om utrusningen har slutat att fungera på rätt sätt.

Konto och lösenordshantering

Lösenord och behörighet till kommunens nätverk och specifika program delas ut vid behov. Nedan följer några enkla riktlinjer att tänka på gällande behörighet och lösenord:

- Lösenord/PIN-kod ska hanteras med samma aktsamhet som t.ex. privata bankkort.
- Lösenord/PIN-kod får inte förvaras på lappar eller på annat sätt finnas tillgängligt i närheten av din dator, telefon eller läsplatta.
- Login och lösenord/PIN-kod får aldrig "lånas ut" eller lämnas till någon annan. Av datatekniska skäl kan det i undantagsfall vara nödvändigt att lämna ut lösenord/PIN-kod till servicedesk eller tekniker. I sådana fall skall lösenordsbyte/PIN-kodsbyte ske omgående efter genomförd åtgärd.
- Lösenord ska konstrueras så att det inte är lätt att avslöja. Man ska inte använda sitt eget eller sina barns namn, bilnummer, telefonnummer eller annat som är lätt att förknippa med enskild användare. Du som enskild användare är personligt ansvarig för vad som händer i systemet med hjälp av din användaridentitet.

Tillträdesskydd

Om du lämnar IT- eller telefonistödet obevakat ska du skydda åtkomsten till enheten genom lösenord på skärmsläckaren eller genom att låsa alternativt logga ut från enheten.

Bärbar utrustning

Se till att du alltid har god uppsyn över bärbar utrustning, såsom mobiltelefoner, bärbara datorer och läsplattor, då den alltid är att betrakta som mycket stöldbegärlig. Bärbar utrustning får aldrig lämnas utan tillsyn. Borttappad eller stulen utrustning ska polisanmälas samt rapporteras till servicedesken alternativt systemstöd.

Kataloger och mappar

I IT-miljön och på datorn finns en mängd kataloger, mappar och filer. När man blir användare får man automatiskt behörighet till H:-katalogen, men i regel också till andra gemensamma kataloger/mappar/filer i IT-miljön.

Det är väsentligt att varje användare har kunskap om hur kataloger/mappar/filer fungerar för att vi ska ha en god ordning i IT-miljön och det är ansvarig chefs ansvar att skapa förutsättningar för detta. Dokument och filer som är inaktuella ska regelbundet rensas för att minska den information som lagras digitalt. Principen är att H: -katalogen enbart ska användas för filer som av olika skäl inte ska vara tillgängliga för andra. C: -katalogen ska aldrig användas för lagring av filer.

Stor restriktivitet bör alltså gälla för att spara filer på H: -katalogen. Bakgrunden till detta är att om en anställd blir borta länge från sitt arbete så har ingen annan tillgång till de filer och den information som ligger på H: -katalogen. Detta kan alltså innebära avsevärda men för verksamheten.

Hantering av USB-minnen och andra lagringsmedia

Känslig information får inte lagras på USB-minnen eller annat externt lagringsmedium om inte informationen är krypterad.

Varje användare är skyldig att vid övergång till annan anställning/uppdrag inom kommunen eller när anställningen/uppdraget upphör se till att H: -katalogen rensas samt att viktiga filer och information överförs på lämpligt sätt till efterträdare eller till förvaltningen.

E-post

Allmänt om kommunicering via e-post

E-post är ett vanligt och bra hjälpmedel för kommunikation både externt och internt. Det finns vissa risker med att skicka uppgifter via e-post som kan vara bra att känna till för att kunna avgöra om e-posten är ett lämpligt medel för kommunicering av den tänkta informationen.

Fel mottagare

Det kan vara svårt att försäkra sig om att endast den avsedda mottagaren tar del av meddelandet. I många fall är det omöjligt att säkerställa identiteten hos en mottagare enbart utifrån en uppgiven e-postadress.

Dagens e-postprogram innehåller också en del funktioner som ökar riskerna för att e-postmeddelanden skickas fel. Det kan vara namn och e-postadresser som fylls i automatiskt eller upprättade e-postlistor som gör att e-posten oavsiktligt riskerar att skickas till fel mottagare eller till betydligt fler mottagare än avsändaren avsett.[1]

Svårt att radera

Det finns vissa säkerhetsbrister i de kommunikationsprotokoll som ligger till grund för e-postsystem. När ett e-postmeddelande skickas mellan e-postservrar över internet passerar det ofta andra servrar på vägen. Om informationen i e-postmeddelandet är oskyddad finns det inget som hindrar att kopior av informationen sparas undan vid var och en av dessa servrar. Kopior av mottagna och skickade e-postmeddelanden ligger ofta kvar i enskilda användares brevlådor både i e-postprogram och i servrar. Det blir då ännu svårare att se till att inte obehöriga tar del av dem, särskilt om e-posten är åtkomlig via ett öppet nät eller är synkroniserad med mobila enheter, till exempel bärbara datorer, läsplattor och mobiltelefoner.

Inget starkt skydd mot yttre intrång

Nynäshamns kommuns e-postsystem är idag inte krypterat och innehåller heller inga andra särskilda skyddsanordningar för att säkerställa att informationen i systemet inte utsätts för yttre intrång.

Postöppning

Här gäller samma regler som för vanlig post. Varje anställd måste kontrollera sin personliga e-postbrevlåda minst en gång om dagen. Samma regler gäller för registrator och övriga som ansvarar för myndighetsbrevlådorna.

Bevakning av brevlådor

Den personliga brevlådan bevakas av innehavaren som vid frånvaro ser till att inkommande meddelanden automatiskt vidaresänds till registratorsbrevlådan eller till någon annan utsedd tjänsteman.

---

[1] Se Datainspektionens hemsida: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/samma-regler-for-alla/hantera-personuppgifter-i-e-post/, den 8 augusti 2018.

Offentlighetsprincipen

För all information som sänds med e-post eller är lagrad i de olika brevlådorna liksom fax, gäller samma offentlighets- och sekretessregler samt arkivregler som för traditionellt sänd post. En offentlighetsprincip för allmänna (offentliga) handlingar gäller enligt tryckfrihetsförordningen samt offentlighets- och sekretesslagen.

Bedömning av e-post

Registrator bedömer e-posten i myndighetsbrevlådan samt de brevlådor som automatiskt kopplas dit. Varje tjänsteman med personlig brevlåda har själv ansvar för bedömningen av sin e-post. Bedömningen av en handlings status är i första skedet att avgöra om den är allmän eller inte allmän. Om man är osäker på om det är allmän handling eller ej ska man prata med eller skicka handlingen till registrator för bedömning. För det fall bedömningen är att handlingen är allmän och ska bevaras ska handlingen skickas den till registrator för registrering.

Allmän handling

Huvudregeln är att handlingar som kommer in är allmänna. Elektroniska handlingar, exempelvis e-post, fax och chatt, anses som inkomna när handlingen är tillgänglig för myndigheten. I de fall där krav ställs på att handlingen är undertecknad för att den ska anses bindande måste den elektroniska handlingen följas av en pappershandling. Det är tidpunkten för den elektroniskt inkomna handlingen som räknas.

Handlingar som skyddas av sekretess

E-postsystemet, faxen eller chatten ska inte användas för överföring av sekretessbelagda handlingar. Använd inte heller e-postsystemet för att skicka känsliga uppgifter som skyddas enligt dataskyddsförordningen, GDPR.

Säker digital kommunikation

Digital kommunicering av integritetskänslig eller sekretessbelagd information får enbart ske via särskilt anpassat system godkänt av IT-enheten.

Integritetskänsliga personuppgifter

Skicka aldrig någon av de särskilda kategorierna av personuppgifter som uppställs i artikel 9.1 GDPR via e-post. Med särskilda kategorier av personuppgifter avses bland annat uppgifter som direkt eller indirekt avslöjar en persons:

- etniska ursprung
- politiska åsikter
- religiösa eller filosofiska övertygelse
- medlemskap i en fackförening
- hälsa
- sexualliv eller sexuella läggning
- genetiska uppgifter och
- biometriska uppgifter som entydigt identifierar personen.

Med genetiska uppgifter avser man sådana uppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken, som t.ex. kan framgå av en dna-analys.

Med biometriska uppgifter anses uppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken som tas fram genom en särskild teknisk behandling, till exempel fingeravtryck.

Uppgifter om lagöverträdelser

Skicka aldrig uppgifter om lagöverträdelser om enskild via e-post. I begreppet lagöverträdelser innefattas brott, fällande domar i brottmål och straffprocessuella tvångsmedel (till exempel häktning, reseförbud, beslag).

Personnummer

Skicka aldrig personnummer via e-post. Personnummer är en integritetskänslig personuppgift. Kommunikation via öppna nät (vilket e-post är) som innehåller personnummer kräver att särskilda säkerhetsåtgärder vidtas.

Anbud

Anbudshandlingar ska inte sändas per e-post eller fax.

Inkommande epostmeddelanden med känsliga uppgifter

Om ett inkommande meddelande innehåller sekretessbelagd information eller integritetskänsliga personuppgifter ska meddelandet utan dröjsmål skrivas ut eller föras in i lämpligt verksamhetssystem och sedan raderas ur e-postsystemet. Se till att även radera meddelandet från papperskorgen.

Handlingar av personlig/privat karaktär

Om meddelanden är av personlig karaktär ansvarar var och en själv för att ta bort dem ur systemet.

Nynäshamns kommun står alltid med som avsändare när e-post skickas.

Expediering av beslut

Om en handling i ett ärende ska expedieras i form av ett e-postmeddelande eller fax krävs en överenskommelse med mottagaren, som dels ska kunna läsa handlingen, dels (om inte handlingen är in scannad) acceptera att ta emot en inte underskriven handling.

Oläsbar post eller bilaga

Om det inte går att läsa det mottagna brevet eller bilagan ska man skicka ett meddelande om detta tillbaka till avsändaren. Varje förvaltning bör ha ett standardbrev att skicka vid dessa tillfällen. I brevet anges vilken/vilka programvaror och versioner ni har möjlighet att läsa. Ta även ut en kopia av det mottagna meddelandet på papper.

Viruskontroll

Stor försiktighet ska tillämpas när e-post har oklar avsändare och eventuellt innehåller HTML-kod eller körbara filer. Var särskilt försiktig med att öppna bilagor om inte avsändaren är känd. Vid minsta osäkerhet bör registrator eller servicedesk kontaktas.

Loggning

I e-postsystemet finns en loggningsfunktion som noterar inkommande och utgående meddelanden. Detta innebär att alla meddelanden kan spåras. Vid behov kan logglista skrivas ut.

Arkivering
Arkivering och aktbildning sker enligt gällande arkivreglemente. Detta gäller såväl inkommande som utgående handlingar.

Att använda e-post i kommunen
Grupputskick till ALLA ska enbart användas för information med omedelbar och direkt anknytning till kommunen och som beror just alla. Ett eventuellt missbruk av e-postfunktionen kan innebära att mailkontot spärras.

Röstbrevlåda
Röstbrevlådans syfte är att öka tillgängligheten både externt och internt. Den måste därför skötas med lika stor omsorg som e-post m.m. Röstbrevlådan skall avlyssnas ofta och minst en gång per dag. I regel får man en avisering per e-post eller sms när meddelande inkommit på röstbrevlådan. Röstbrevlådan ska stängas av om man inte kan lyssna av den under t.ex. semesterledighet.

Sociala medier
"Kommunens riktlinjer för sociala medier" ska följas vid användning av sociala medier.

Ersätter
Riktlinjer för IT-användning och telefonistöd i Nynäshamns kommun, daterad 2015-03-20.

Diarienummer
KS/2018/0210/005-6

Datum
2018-08-08

Upprättad av
Per Österberg, IT-chef samt Yvonne Persson, kommunjurist

Granskad/beslutad av
Tommy Fabricius, kommundirektör

Version
2