

Anvisning

vid lån och användning av digital utrustning för
förtroendevalda

2022-10-01 – 2026-12-31



Innehållsförteckning

1.	Användning av digital utrustning för förtroendevalda	2
1.1	Kommunens egendom	2
1.2	Syfte och användande	2
1.2.1	Kallelse och handlingar	2
1.2.2	E-post	2
1.2.3	Privat användning.....	3
2	Säkerhet.....	3
2.1	Förvaring	3
2.2	Lås dina enheter.....	3
2.3	Lösenord.....	3
3	Utlämning av digital utrustning.....	4
4	Om erhållen digital utrustning.....	4
4.1	Trådlöst nät och mobil uppkoppling.....	4
4.2	Sekretesshandlingar	5
4.3	Loggning.....	5
4.4	Stöld eller förlust	5
4.5	Support – vad ingår?.....	5
4.6	Utbildning.....	5
5	Återlämning av digital utrustning	6
5.1	Radera utrustningens innehåll	6
6	Anvisningar gällande informationssäkerhet.....	7

1. Användning av digital utrustning för förtroendevalda

I Sollefteå kommun läser förtroendevalda främst de dokument som behövs för uppdraget digitalt. För att möjliggöra detta tillhandahåller kommunen digital utrustning. Riktlinjerna beskriver vad som gäller vid lån av digital utrustning.

1.1 Kommunens egendom

Den utrustning som utlånas ägs av kommunen. Det innebär att den ska hanteras med omsorg och försiktighet eftersom den ska återlämnas efter avslutat uppdrag eller vid utbyte till ny utrustning.

Om utrustningen under lånetiden förloras ska låntagaren omedelbart anmäla detta till kansliet.

1.2 Syfte och användande

Huvudsyftet med lånet är att kunna ta del av dokument och information som behövs för uppdraget. Genom digitalisering blir hanteringen av handlingar effektivare samtidigt som spårbarhet och säkerhet ökar.

1.2.1 Kallelse och handlingar

Förtroendevald får tillgång till kallelser och handlingar inför sammanträden via Platina Meetings.

1.2.2 E-post

I kontakt mellan kommunen och förtroendevalda används den kommunala e-posten. E-posten ska därför öppnas regelbundet.

När du använder din e-post gäller samma regler som för anställda i Sollefteå kommun vad gäller till exempel informationssäkerhet, allmänna handlingar och GDPR.

Du får inte skicka sekretessbelagd eller känslig information via din e-post. Minska risken för att bli utsatt för bedrägeri genom att låta bli att klicka på länkar eller bilagor från okända avsändare. Ladda heller inte ned program som kommer via e-post, sms eller olika webbsidor, särskilt när avsändare är okänd. Anvisningar för informationssäkerhet och GDPR [finns att läsa på KomIn](#).

Samma offentlighets-, sekretess- och arkivregler gäller för e-post som för papperspost. Var och en som sänder eller tar emot e-post måste själv bedöma om en försändelse är allmän handling och om den därmed ska vidarebefordras till nämndens/styrelsens diarium.

Sekretesskyddade uppgifter ska inte skickas över e-postsystemet eller på annat sätt via internet. Skulle ändå en sekretesshandling inkomma i e-posten ska kontakt tas med kansliet för att få hjälp.

Upplys avsändaren att fortsättningsvis inte använda sig av e-post för sekretess.

Vidaresänd inte e-post innehållande sekretess.

1.2.3 Privat användning

Den digitala utrustningen får även användas privat under förutsättning att kommunens policy och anvisningar följs och det inte påverkar dess huvudsyfte. Kommunen har inte ansvar för privat data eller privat valda applikationer som laddats ner eller sparats.

Utrustningen får inte lånas ut till annan person för användning.

2 Säkerhet

2.1 Förvaring

Förtroendevalda har ansvar för att ingen obehörig får åtkomst till utrustningen och dess information. Det är därför viktigt att den förvaras på ett säkert sätt och inte lämnas obevakad på allmän plats.

2.2 Lås dina enheter

Du behöver skydda informationen när du arbetar med känslig information, på dator, surfplatta eller mobiltelefon. Det innebär att du alltid måste låsa enheterna när du lämnar dem eller vid förvaring i hemmet. Ingen annan ska ha tillgång till enheterna eller kunna ta del av informationen.

2.3 Lösenord

Enheten skyddas med lösenkod och automatisk låsning sker efter viss tid av inaktivitet. Förtroendevald är personligt ansvarig för att inte obehöriga kommer åt lösenord, enhet eller information.

Ett säkert lösenord för e-post innehåller bokstäver, siffror och gärna specialtecken.

Bygg upp lösenordet på ett sätt så att det är lätt för dig att komma ihåg det, men svårt för andra att knäcka det.

Användaren förbinder sig att inte lämna ut koden eller lösenord till andra och inte heller förvara utrustningen så att de blir åtkomliga för andra.

3 Utlämnning av digital utrustning

Vid utlämnande av ny digital utrustning kvitteras en blankett där det framgår vilken utrustning som utlånats. Genom att skriva på denna blankett förbinder sig förtroendevald att följa de anvisningar som gäller för kommunens IT-utrustning samt kommunens policy för informationssäkerhet och dataskydd. [Dessa policys och anvisningar finns att ta del av på KomIn.](#)

Vid tillfälle för mottagande och kvittens av digital utrustning ges information om användar-id, lösenord, e-postadress samt inloggningsuppgifter för att läsa handlingar till sammanträden.

4 Om erhållen digital utrustning

Enheten registreras i kommunens MDM (Mobile Device Management) och där ges åtkomst till det som behövs för utövande av uppdraget.

Förtroendevald har automatiskt tillgång till följande:

- Kommunens trådlösa nätverk.
- Platina Meeting för att läsa/anteckna i dokument till sammanträden
- Digital signering
- Tillgång till e-post/kalender som förtroendevald.
- Länk till Sollefteå kommuns hemsida/intranät (Komin).
- Pdf-läsare Acrobat Reader.

Följande koder och konton med tillhörande lösenord är nödvändiga för användandet av den digitala utrustningen:

- **Pinkod** för SIM-kortet - behöver anges när surfplattan slås på efter att strömmen varit bruten.
Förtroendevald ansvarar för PIN och PUK-kod på SIM-kortet.
SIM-kortet i enheten får inte bytas mot annat för privat bruk.
- **Skärmkod** är förinställt.

4.1 Trådlöst nät och mobil uppkoppling

Surfplattan ska, om möjligt, kopplas upp mot ett betrott trådlöst nätverk när det finns tillgängligt. Exempelvis i egna hemmet eller i Sollefteå kommuns verksamheter. Undvik att ansluta mot okända nätverk, exempelvis när du befinner dig på ett hotell eller café som erbjuder wifi utan lösenordsskydd. Möjlighet kan finnas för obehöriga att komma åt din information utan att du är medveten om det.

På den modell av surfplatta som kommunen tillhandahåller finns även SIM-kort för att koppla upp den mot det mobila nätet. Kommunen bekostar SIM-kort till förtroendevalda. Surf genom mobilnätet är avsett för det politiska uppdraget och abonnemanget innehåller en fast surfmängd per månad.

Abonnemanget är spärrat för surf utanför Europa.

Känslig eller sekretessbelagd information diskuteras inte annat än via anvisad plattform, med anledning av att informationen kan avlyssnas.

4.2 Sekretesshandlingar

Sekretesshandlingar skickas enligt anvisningar från kansliet.

4.3 Loggning

Användning av kommunens utrustning loggas avseende vem som nyttjat den, vilka webbplatser som besöks etc. Loggar kan användas vid misstanke om otillbörlig användning.

4.4 Stöld eller förlust

Vid stöld eller förlust av digital utrustning ska detta meddelas till kansliet.

Vid misstanke om stöld ska det även anmälas till polisen och bekräftelsen på anmälan lämnas till kommunen. Ärendenummer efter anmälan lämnas till kansliet.

SIM-kortet spärras via operatören (Telia) av dig som förtroendevald.

4.5 Support – vad ingår?

Kansliet ger användarsupport för funktionerna såsom Platina Meetings eller andra - till uppdraget - tillhörande applikationer.

IT, via 0620 -68 23 00, ger övrig support om det uppstår problem med din digitala utrustning, t ex återställning/fabriksåterställning eller vid behov av reparation/utbyte.

4.6 Utbildning

Utbildning erbjuds förtroendevalda på följande sätt:

- Genomgång av tillhandahållen utrustning sker genom kontakt med kansliet.
- Stöd/utbildning av Platina meetings, e-post mm tillhandahålls av personalen på kansliet.
- [Webbaserad utbildning inom informationssäkerhet och dataskydd.](#)

5 Återlämning av digital utrustning

Förtroendevald ska omgående efter avslutat uppdrag återlämna digital utrustning samt de tillbehör som tillhör kommunen. Återlämnandet sker till kansliet. Om inte detta sker kan Sollefteå kommun kräva ersättning för utrustningen.

Återlämnandet kvitteras på samma blankett som användes vid utlåningen.

5.1 Radera utrustningens innehåll

Vid återlämnandet ansvarar låntagaren för att utrustningens innehåll raderas.

Observera att när allt innehåll raderas försvinner även alla eventuella bilder och andra typer av filer. Dessa måste sparas på annan plats om de ska behållas.

6 Anvisningar gällande informationssäkerhet

Informationssäkerhets- och dataskyddspolicy

Anvisning informationssäkerhet och dataskydd

Anvisning informationsklassning

Anvisning, regler för IT-användare

Anvisning för informationssäkerhet vid distansarbete

Ovanstående finns att finna på följande sida;

[Informationssäkerhet - Komin \(solleftea.se\)](https://www.solleftea.se/komin/informationssakerhet)