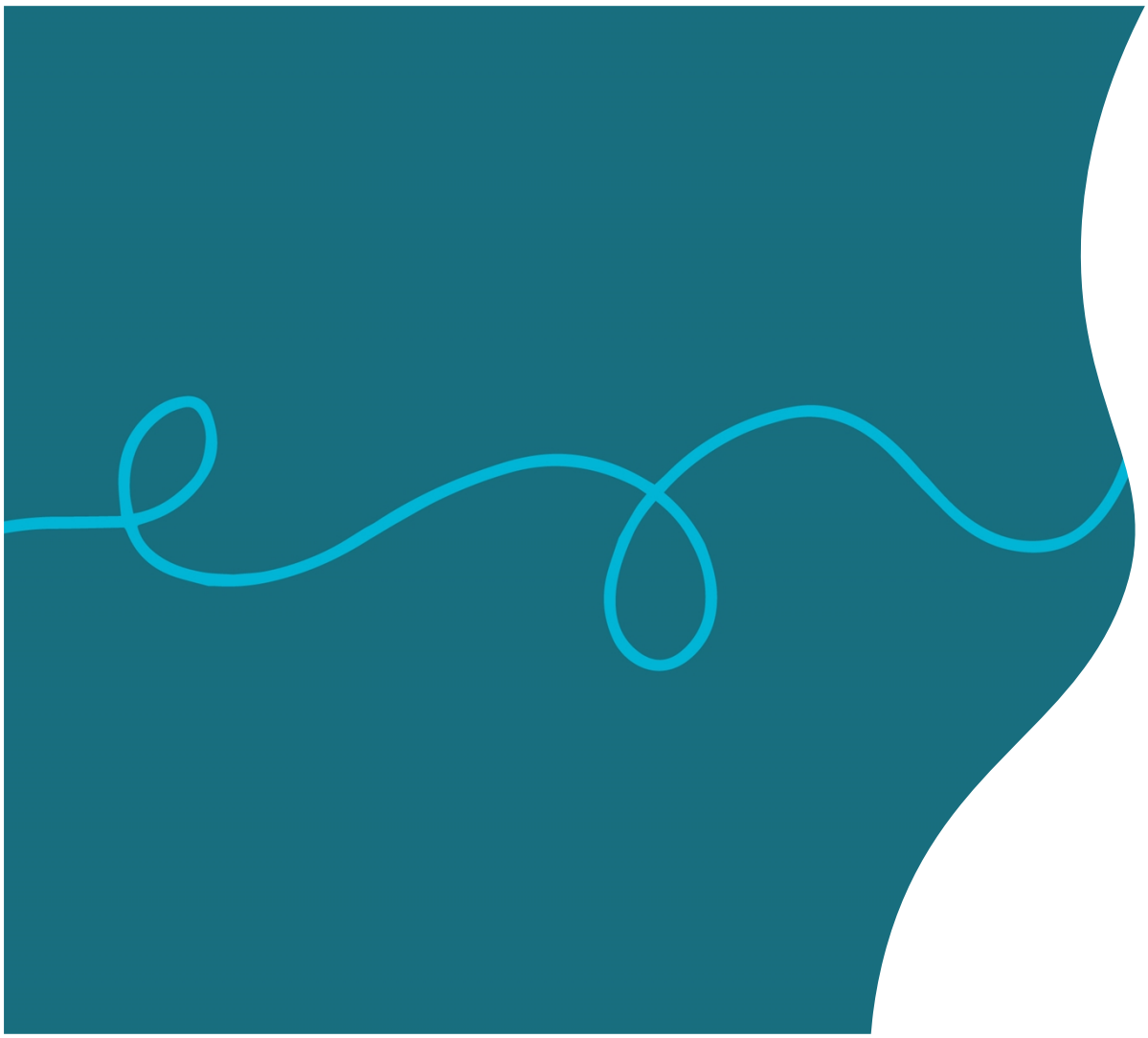
Dokumenttyp: Riktlinje
Diarienummer: KS-2024/585

Beslutande nämnd: Kommunstyrelsen



Riktlinjer för mobila enheter

Beslutsdatum: 2025-MM-DD
Giltighetstid: 2029-12-31
Dokumentansvarig: Informationssäkerhetssamordnare
Kontor: Kommunledningskontoret

Knivsta kommun

Innehållsförteckning

Inledning

Denna riktlinje omfattar alla slutanvändare i Knivsta kommun och gäller för alla former av mobila enheter som tillhandahålls av kommunen till medarbetare, förtroendevalda eller elever.

Syfte

Syftet är att säkerställa att mobila enheter används på ett säkert och ansvarsfullt sätt. Riktlinjen förtydligar den enskildes ansvar och ger vägledning kring vad som är tillåtet eller otillåtet att göra med kommunens mobila enheter.

Omfattning

Riktlinjen gäller alla medarbetare i Knivsta kommun som använder någon form av mobil enhet i tjänsten. Alla som får tillgång till en mobil enhet ansvarar för att den används korrekt enligt riktlinjen.

Definition av mobil enhet

Med mobil enhet avses exempelvis bärbara datorer, mobiltelefoner, surfplattor, läsplattor och liknande, samt externa tillbehör som hörlurar, tangentbord, muspekare, extern lagringsmedia och liknande.

Användning av mobil enhet

Distansarbete

Var extra försiktig med dina mobila enheter vid distansarbete. Undvik offentliga platser och använd sekretessfilter om du måste arbeta med konfidentiell information i sådana miljöer.

Frånvaro eller avslut

Vid avslut av anställning, förtroendeuppdrag eller skolgång ska alla mobila enheter återlämnas till kommunen. Vid längre frånvaro eller föräldraledighet beslutar närmsta chef om enheterna ska återlämnas tillfälligt.

Förvaring

Mobila enheter ska alltid förvaras säkert. När du inte använder dem, håll dem i ett låst utrymme där de inte syns. På arbetsplatsen eller när du jobbar hemifrån, aktivera skärmlåset om du lämnar enheten obevakad. I offentliga miljöer får du aldrig lämna mobila enheter utan uppsikt.

Incidenthantering

Misstänker du skadlig programvara eller nätfiskeförsök, meddela IT-Centrum omedelbart enligt kommunens incidenthanteringsrutin. Vid stöld eller förlust av en mobil enhet, följ gällande rutin för stöld av IT-utrustning.

Lösenord

IT-Centrum lösenordsanvisning ska följas. Mobiltelefoner ska skyddas med ansiktsigenkänning eller fingeravtrycksavläsning och mobila enheter ska alltid skärmlåsas när de inte används. Vid användning av Apple-enheter ska ett särskilt Apple-ID skapas kopplat till medarbetarens anställning. Privata Apple-ID får inte användas. En medarbetare kan använda samma Apple-ID på flera Apple-enheter.

Nätverk

När du är ansluten till kommunens VPN är du skyddad av kommunens brandväggar. Detta skydd gäller inte på andra nätverk, som ditt hemnätverk eller offentliga nätverk. Därför ska du alltid vara ansluten till kommunens VPN när du arbetar hemifrån eller använder offentliga nätverk.

Privat användning

Du representerar alltid kommunen när du använder kommunens mobila enheter. Använd aldrig din knivsta.se-mejladress privat eller din privata mejladress i

tjänsten. Nödvändiga privata telefonsamtal, SMS/MMS och privat surf är tillåtna i rimlig omfattning, och löpande under tjänsteresor. Dual SIM är inte tillåtet.

Privat utrustning

När du arbetar på distans får du använda privat utrustning som är trådbunden. I andra fall ska du använda den utrustning som du har fått av arbetsgivaren, både trådlös och trådbunden. Privata smarta enheter och extern lagringsmedia får aldrig kopplas till kommunens mobila enheter. På arbetsplatsen får du inte använda privat utrustning med kommunens enheter.

Programvara

Ändra aldrig enhetens grundfunktioner och installera säkerhetsuppdateringar så fort som möjligt. Du får inte installera uppenbart privata appar på din mobila enhet.

Förvaltning

Kommunstyrelsen ansvarar för att informera om riktlinjen. Alla nämnder ansvarar för att implementera och följa riktlinjen.

Knivsta kommun