

IT- och digitaliseringsenheten

IT-användarpolicy

för Bengtsfors-, Färgelanda- och Åmåls kommun

Kommunens IT-utrustning ska användas ansvarsfullt, säkert och lagenligt, i enlighet med kommunens värdegrund och gällande lagstiftning.

Detta dokument består av policy, riktlinjer och regler. Policyn beslutas av kommunfullmäktige och anger övergripande inriktning. Riktlinjer beslutas av kommunstyrelsen och preciserar policyn. Regler beslutas i enlighet med respektive kommuns beslutsordning.

Riktlinjer

Syfte

Att fastställa riktlinjer för användning av datorer, mobiltelefoner, surfplattor, programvaror och annan IT-teknisk utrustning som tillhandahålls av kommunen. Målet är att säkerställa att utrustningen används på ett säkert och ansvarsfullt sätt.

Ansvar

Nämnd- och bolagsstyrelser ska säkerställa att kommunens IT-användarpolicy efterlevs.

Nämnd- och bolagsstyrelser ska säkerställa att kommunens IT-användarpolicy finns tillgänglig för IT-användare.

IT-användare ansvarar för att följa policyn med riktlinjer och regler.

Omfattning och definition

Med IT-användare avses alla kommunanställda och förtroendevalda i Bengtsfors-, Färgelanda- och Åmåls kommun som brukar IT-utrustning som tillhandahållits av kommunen. Det gäller även för den med annan typ av uppdrag för kommunens räkning, som konsultuppdrag eller frivilligt uppdrag där man tilldelats

IT-utrustning eller användarkonto. För elever gäller ett separat användaravtal som upprättas mellan elev, vårdnadshavare och skola.

Med **IT-utrustning** avses all teknisk utrustning som används för att skapa, bearbeta, lagra, överföra eller visa information inom kommunens verksamheter.

Begreppet omfattar bland annat:

- stationära och bärbara datorer, surfplattor och mobiltelefoner,
- servrar, lagringsenheter och nätverksutrustning,
- skrivare, skannrar och annan kringutrustning,
- digitala mötes- och presentationssystem,
- hårdvara i verksamhetsspecifika system (t.ex. sensorer, styr- och övervakningsutrustning), samt
- tillhörande tillbehör och säkerhetskomponenter som används för inloggning, identifiering eller dataskydd.

IT-utrustning omfattar både kommunägd, leasad eller på annat sätt tillhandahållen utrustning.

Tillåten användning

IT-utrustning och digitala resurser är till för att stödja kommunens verksamhet och ska användas på ett **ansvarsfullt, säkert och lagenligt sätt**.

Grundprinciper

IT-utrustning ska användas för **arbetsrelaterade ändamål** och inom ramen för den anställdes eller uppdragstagarens **arbetsuppgifter och behörighet**.

Privat användning får endast ske i **begränsad omfattning**, under förutsättning att det inte:

- påverkar arbetet eller verksamhetens drift,
- medför kostnader för kommunen,
- orsakar säkerhetsrisker, eller
- bryter mot lag eller kommunens styrdokument.

Fjärranslutning och hemarbete

Det är möjligt att använda IT-utrustning för att på distans ansluta till kommunens lagringsytor, IT-system m.m. Detta får ske och är en naturlig del av det moderna hybridarbetet, men det får endast ske genom att användaren uteslutande använder den utrustning som kommunen har tillhandahållit.

Användaren ska också följa de regler och rutiner för digital informationshantering, informationssäkerhet och dataskydd som antagits av respektive kommun. I dessa regleras exempelvis användarens ansvar för att säkerställa användning av säkra internetanslutningar och att obehöriga inte kan ta del av skyddsvärd information.

Kunskap, regler och försiktighet

Det är användarens skyldighet att hålla sig informerad samt ta del av de utbildningar, rutiner, riktlinjer och andra styrande dokument som tas fram och sprids av kommunen för att säkerställa trygg användning av IT-utrustning och IT-system. Om osäkerhet kring vilka regler eller arbetssätt som gäller, ska användaren ta kontakt med sin närmaste chef, för information.

Såväl myndigheter som privatpersoner utsätts fortlöpande för bedrägligt beteende via internet och e-post. Externa angripare försöker på detta sätt få tillgång till information, utnyttja säkerhetshål eller för ekonomisk vinning. Det är användarens skyldighet att vidta försiktighet och inte klicka på tveksamma länkar eller uppge inloggningsinformation för obehörig. Vid tveksamhet är det alltid bäst att vända sig till IT-support eller närmaste chef för stöd vid denna typ av bedömningar.

Vid avslutande av anställning

Vid avslut av anställning, uppdrag eller konsulttjänst ska användarens åtkomst till kommunens IT-system, nätverk och informationstillgångar omedelbart avslutas eller justeras.

Den närmaste chefen ansvarar för att:

1. Informera HR-enheten/avsluta anställningen i personal/lönesystem för att säkerställa att anställningen upphör på korrekt sätt och vid rätt tidpunkt, vilket i sin tur styr konto för IT-behörigheter och åtkomst till kommunens IT-miljö.

2. Säkerställa att all IT-utrustning, inklusive dator, surfplatta, mobiltelefon, passerkort, säkerhetsdosa, USB-minnen och annan digital utrustning som tillhandahållits av kommunen, återlämnas i fungerande skick.
3. Besluta om hantering av lagrade filer, e-post och annan digital information som kan ha fortsatt verksamhetsrelevans.
4. Kontrollera att privat information på kommunens utrustning har raderats på ett korrekt sätt och att verksamhetsrelaterad information bevaras enligt gällande dokumenthanteringsplan.

Efter avslutad anställning eller uppdrag är det inte tillåtet för den före detta användaren att på något sätt använda, kopiera, sprida eller på annat sätt utnyttja kommunens information, system eller licenser.

Regler

Säker och korrekt användning

Användaren ska:

- följa gällande säkerhetsrutiner, policyer och instruktioner,
- skydda sina **användaruppgifter, lösenord och åtkomstmedel,**
- se till att IT-utrustning inte används av **obehöriga personer,**
- hantera information och data i enlighet med **lagstiftning och sekretessbestämmelser,**
- omedelbart rapportera **incidenter, misstänkta säkerhetsbrott eller felaktig användning** till ansvarig chef eller IT-funktion.

Otillåten användning

Grunden för vad som är otillåten användning av IT-utrustning är att användningen inte får påverka kommunen negativt. Detta omfattar såväl extra kostnader och merarbete som inte annars skulle uppstå, negativ påverkan på allmänhetens uppfattning om kommunen (förtroendeskadlig påverkan) samt vad som omfattas av lagstiftning. Med negativ påverkan omfattas också användande som påverkar kommunens IT-säkerhet/informationssäkerhet negativt.

Med utgångspunkt i grundprincipen om att det inte är tillåtet att avsiktligt eller genom tydlig oaktsamhet påverka kommunen negativt, är det många gånger sunt förnuft och en egen bedömning som behövs göras. Följande punkter är exempel på otillåten användning:

- Det är förbjudet att ladda ner, installera eller använda programvara som inte är godkänd av IT- och digitaliseringsenheten.
- Det är förbjudet att medföra extern IT-teknisk utrustning eller kringutrustning till arbetsplatsen och ansluta den till dator, surfplatta, smartphone, fast nätverk, skrivare eller annan IT-teknisk infrastruktur som kommunen ansvarar för. Detta gäller också lagringsmedia som användaren kan ha fått på mässor, från extern part o. dyl.
- Privat IT-utrustning ska som generell regel inte anslutas till kommunens IT-utrustning, nätverk eller system. I synnerhet inte utrustning med lagringskapacitet, exempelvis privata USB minnen, externa hårddiskar, minneskort eller annan privat lagringsmedia.

Viss privat kringutrustning av passiv karaktär får i normalfallet användas i begränsad omfattning, under förutsättning att utrustningen saknar egen lagring och mjukvara. Ansluten utrustning får inte påverka informations-säkerheten negativt. Exempel på sådan tillåten kringutrustning är headset eller hörlurar, tangentbord, mus samt extern bildskärm. Vid osäkerhet ska användaren samråda med närmaste chef eller IT- och digitaliserings-enheten innan utrustningen tas i bruk. Privata mobiltelefoner, surfplattor och annan aktiv utrustning får inte fysiskt anslutas, om detta inte uttryckligen har godkänts. Undantag får endast medges efter förhandsgodkännande av IT- och digitaliseringsenheten, baserat på en dokumenterad bedömning av informations- och IT-säkerhetsrisk.

- All IT-utrustning och programvara/licens ska beställas och köpas in genom IT- och digitaliseringsenheten.
- All typ av upphovsrättsskyddat material är förbjudet att hantera utan tillstånd på kommunens tekniska utrustning. Det innefattar bland annat piratkopierad musik, film eller program.
- Användning av utrustningen för olagliga aktiviteter, inklusive men inte begränsat till, spridning av skadlig programvara, är strängt förbjudet. Alla brottsliga handlingar kommer polisanmälas.

- E-postadress som tilldelas användaren för att utföra ett arbete/uppdrag är ett arbetsredskap. Den ska uteslutande användas för arbetsuppgifter och professionella kontakter. Användaren ska inte använda den för privat korrespondens, i sociala medier eller för att registrera sig på internetsidor/tjänster för privat bruk.

Otillåtna typer av innehåll

Kommunens IT-utrustning, nätverk och digitala plattformar får inte användas för att skapa, lagra, sprida eller visa innehåll som är **olagligt, oetiskt eller oförenligt med kommunens värdegrund**.

Otillåtet innehåll omfattar bland annat:

1. Olagligt innehåll

- Material som strider mot svensk lag, exempelvis:
 - barnpornografiskt material,
 - hets mot folkgrupp, hot eller förtal,
 - upphovsrättsskyddat material som används eller sprids utan tillstånd,
 - dataintrång, sabotage eller annan otillåten åtkomst till IT-system,
 - spridning av skadlig kod, virus eller annan IT-relaterad brottslighet.

2. Stötande eller oetiskt innehåll

- Material som kan uppfattas som kränkande, diskriminerande, trakasserande eller på annat sätt strider mot kommunens värdegrund.
- Pornografiskt eller våldsamt material.
- Innehåll som syftar till eller uppmuntrar till kriminell verksamhet.

3. Politiskt, kommersiellt eller privat innehåll

- Spridning av politisk propaganda, kommersiell reklam eller religiös påverkan i tjänstesammanhang.
- Material kopplat till privata affärsintressen, nätförsäljning eller annan verksamhet utanför kommunens uppdrag.
- Användning av kommunens kommunikationskanaler (t.ex. e-post, chatt, webb) för privat opinionsbildning eller personliga konflikter.

4. Osäkert eller otillåtet tekniskt innehåll

- Installation eller användning av oauktoriserade program, appar, tillägg eller script.
- Filer eller länkar som kan äventyra kommunens IT-säkerhet, till exempel genom phishing, malware eller otillåtna molntjänster.

Om användaren är osäker kring användning av utrustningen, t. ex. om användaren i tjänsten behöver besöka en hemsida som normalt skulle kunna anses vara olämplig, ska användaren föra dialog med chef innan detta sker. Många sidor är blockerade på central nivå och önskar en användare få tillgång till en sådan sida måste dialog föras med IT- och digitaliseringsenheten.

Ansvar och underhåll

- Användaren är ansvarig för att hålla utrustningen i gott skick och ska rapportera eventuella problem och skador till IT-supporten omedelbart.
- Misstänker användaren att utrustningen utsatts för skadlig programvara ska detta rapporteras till IT-supporten omedelbart.
- Utrustningen ska skyddas mot stöld och skada, vilket särskilt ställer krav på den användarens aktsamhet och omdöme då utrustning tas med hem eller transporteras.
- Lösenord/nycklar är personliga och får inte delas med andra.
- Information som hanteras på kommunens tekniska utrustning ska skyddas, användaren får aldrig lämna utrustningen inloggad utan tillsyn.

Övervakning och integritet

Enligt gällande lagstiftning, bland annat Arbetsmiljölagen och Dataskyddsförordningen, tillsammans med EU-direktiv, NIS2 och CER, har kommunen rätt att övervaka användningen av sin tekniska utrustning för att säkerställa att den används i enlighet med gällande lagar samt dessa riktlinjer. Detta för att förebygga och upptäcka bland annat riskfyllt eller ovälkommet beteende, kränkande särbehandling och illojalitet men också för att säkerställa att kommunens tekniska utrustning och information inte hanteras på ett olovligt eller olagligt sätt.

Övervakning och behörighetsstyrning sker på flera nivåer, bland annat genom regler i brandväggarna och loggning av trafik. Den data och information som

skapas på kommunens tekniska utrustning tillhör kommunen, det gäller bland annat dokument och filer, mail och program som användaren har producerat.

Detta innebär att kommunen, i det fall en användare inte kan eller vill medverka för att tillgängliggöra filer eller e-postmeddelanden som lagras på kommunens utrustning, självständigt kan plocka fram dessa för att verksamheten inte ska påverkas negativt. Exempelvis kan detta ske vid plötslig eller långvarig sjukdom eller då användaren är förhindrad att tjänstgöra.

I möjligaste mån ska kommunen söka användarens medverkan i dessa fall, med hänvisning till användarens integritet, men ett dokumenterat samtycke är inte nödvändigt. Vid avslut av anställning får inte data och information tas med ut från verksamhetens system om det inte är godkänt av chef.

Användaren ska vara medveten om att kommunen kommer granska användningen av utrustningen om man misstänker att en användare missbrukar eller bryter mot dessa riktlinjer. Innan granskning ska chef med personalansvar samt HR vara med i utredningen. Att kontrollera användning bör inte vara det första alternativet, för att värna om användarens integritet. Undantagsfall är vid misstanke om brott då man skyndsamt bör kontrollera och dokumentera.

Påföljd och ekonomiskt ansvar

Olyckshändelser i arbetet kan ske och IT-utrustning kan skadas även vid normal användning och iakttagande av försiktighet. Om en användare däremot bryter mot användaravtalet eller agerar genom grov eller upprepad oaktsamhet, kommer kommunen att agera genom proportionerlig påföljd.

Sådan påföljd kan i mindre allvarliga fall ske i form av dokumenterad, skriftlig varning och/eller löneavdrag för den utrustning som måste repareras/ersättas. I allvarliga fall, exempelvis där kommunen lider allvarlig ekonomisk skada, grav förtroendeskada eller om kriminella handlingar begås med hjälp av kommunens utrustning, kan förutom polisanmälan också krav på skadestånd väckas, samt process för ytterligare arbetsrättsliga åtgärder inledas.