Diarienummer: KS 2018/02272

Program
Policy
Handlingsplan
**Riktlinje**

# Riktlinje för användning av digitala verktyg och telefonitjänster i Västerås stad

Beslutad av Digitaliseringsdirektören

25 november 2021

VERSION 2.0 • 2021-11-25

VÄSTERÅS STAD

**Innehållsförteckning**



| | |
|---|---|
| Program | uttrycker värdegrunder och förhållningssätt för arbetet med utvecklingen av Västerås som ort inklusive koncernen Västerås stad |
| Policy | uttrycker värdegrunder och förhållningssätt för arbetet i koncernen Västerås stad |
| Handlingsplan | anger strategier och konkreta åtgärder för att nå den politiska viljeinriktningen och fastställda mål på olika nivåer i organisationen |
| Riktlinje | säkerställer ett riktigt agerande och en god kvalitet i handläggning och utförande i koncernen Västerås stad |

# Riktlinje för användning av digitala verktyg och telefonitjänster i Västerås stad

Dessa riktlinjer gäller för användare (medarbetare/elever/brukare) som nyttjar digitala arbetsplatser, digitala lösningar, smarta telefoner och elektroniska kommunikationer i Västerås stad. Riktlinjerna gäller även förtroendevalda, tillfällig personal och samarbetspartners.

# 1. Utgångspunkter och generella regler

## 1.1. IT-utrustningen är arbetsredskap

En grundläggande utgångspunkt är att digitala arbetsplatser och digitala lösningar som tillhandahålls av Västerås stad är redskap för arbetet och ska hanteras på sådant sätt. Det är inte tillåtet att ladda ner, kopiera och/eller lagra upphovsrättsligt material för privat bruk på stadens utrustning inklusive mobiltelefoner och externa lagringsmedia.

## 1.2. Användarens ansvar

Användaren bör inte själv installera andra programvaror på sin utrustning än de som tillhandahålls eller godkänns av Västerås stad.

Om så ändå görs är det under eget ansvar och man behöver i så fall ta större eget ansvar för den support och underhåll som kan uppstå. Det innebär också att man ökar riskerna för informationsförlust och andra säkerhetsrelaterade risker.

Användaren har förtroende att efter eget gott omdöme använda sig av utrustningen på ett ändamålsenligt sätt. Riktlinjerna innebär inte ett generellt förbud mot privat användning utan viss sådan användning får ske, men endast i begränsad omfattning och då i enlighet med dessa riktlinjer. Användaren ansvarar för att skydda utrustningen mot stöld och otillbörligt användande.

Vid misstanke om att IT-utrustning blivit stulen eller på annat sätt har förkommit ska detta omedelbart rapporteras till Service Desk (Kundtjänsten för IT) som därefter ger användaren information om vilka ytterligare åtgärder som behöver vidtas, exempelvis att göra polisanmälan.

Användaren ansvarar för att hantera och vårda tilldelad IT-utrustning så att den är fungerande under hela sin livslängd till planerat utbyte enligt stadens beslutade rutiner. Vid eventuellt utbyte av IT-utrustning i förtid kommer den i första hand att ersättas med likvärdig begagnad utrustning.

Datorer som ej används skall vara avstängda. Detta gäller när användaren går hem för dagen, om inte annat anvisats.

IT-utrustningen får inte användas för olagliga eller annars olämpliga aktiviteter, till exempel för att sprida virus eller annat skadligt material, eller på annat sätt störa eller skada IT-säkerheten.

Det är inte tillåtet att använda någon annans användaridentitet eller att låna ut sin behörighet. Principen säger att varje användare ska använda ett eget användarkonto. Gruppkonton får inte användas annat än i undantagsfall.

### 1.3. Mer information

Ansvaret för uppföljning av dessa riktlinjer finns beskrivet i ”Riktlinje för Informationssäkerhet”.

På Insidan finns instruktioner, användarhandledningar och ytterligare information samlad.

# 2. Tillämpning av riktlinjerna inom Västerås stad

### 2.1. Lösenord

Lösenord till IT-systemen är personligt och omfattas normalt av sekretess enligt 18 kap 8 § Offentlighets- och sekretesslagen (2009:400), OSL. Lösenord ska helst omfatta sexton tecken men minst åtta tecken och vara svåra att gissa sig till av andra personer. Lösenord bör innehålla en blandning av versaler, gemener, siffror och specialtecken. De kan vara långa ihopsatta ramsor som är enkla att komma ihåg (exempelvis *Jannefyller40!Januari* som dock inte bör användas eftersom det står här. Välj en annan ramsa). Undvik lösenord som kan associeras med din person, egennamn samt vanliga ord, till exempel, sommar, vinter etc. Skriv aldrig ner eller lagra lösenordet i klartext. För elever gäller separat rutin.

För surfplattor och telefoner är kravet att lösenordet, (PIN-koden) ska vara minst fyra tecken.

Lämna aldrig ut lösenordet till någon. Vid misstanke om att lösenordet har avslöjats för andra ska lösenordet omgående bytas ut och Service Desk kontaktas. Lösenord ska bytas när systemet uppmanar till detta, vilket i regel sker med 90 dagars mellanrum. Tänk på att även byta ut lösenord på externa webbplatser eller andra system som inte tillhör staden, till exempel på externa arbetsytor. Återanvänd inte ditt nätverkslösenord i staden för dessa inloggningar.

Läs mer om byte av lösenord på Insidan.
(https://insidan.vasteras.se/organisation/digitalisering/informationssakerhet/losenord-och-losenordsbyte/Sidor/default.aspx)

Obevakad IT-utrustning ska alltid vara låst för att förhindra obehörig användning. Skärmlåset på stadens datorer aktiveras automatiskt efter 10 minuter, men användaren ska aktivt låsa datorn när den lämnas obevakad. Telefoner och

surfplattor ska ha automatisk låsning aktiverad, denna funktion får inte avaktiveras.

## 2.2. Informationssökning i verksamhetssystem

Informationssökning i verksamhetssystem får bara ske i den utsträckning det är nödvändigt för att kunna utföra arbetsuppgifterna. All annan sökning är otillåten och kan komma att ses som dataintrång. Med verksamhetssystem avses till exempel personalsystem, ekonomisystem, administrativa system med dokumentation om sökande, brukare, elever och liknande.

## 2.3. Internet

Alla aktiviteter på Internet med stadens utrustning är spårbara.

Användare som är aktiva på Internet ska vara medvetna om att aktiviteterna som görs kan påverka allmänhetens uppfattning om Västerås stad som organisation och förtroendet för dig som tjänsteman. Det är därför särskilt viktigt att som representant för Västerås stad beakta god etik och gott omdöme på Internet.

All Internettrafik och e-post loggas centralt. Västerås stad har som arbetsgivare/uppdragsgivare rätt att, utan att meddela användaren, gå igenom dessa loggar för att kontrollera efterlevnad av regler, lagstiftning och riktlinjer.

**Vid användning av Internet gäller följande:**

Användare får i begränsad omfattning använda Internet för privata syften.

Filmer och program, material som innebär intrång i annans upphovsrätt, inklusive spel eller andra utrymmeskrävande filtyper får inte för privat bruk laddas ned, lagras eller spridas i eller via Västerås stads nätverk.

Sociala medier, t ex Facebook, Twitter, Bloggar LinkedIn, m.fl., kan vara värdefulla verktyg i arbetet. Var alltid tydlig med om du kommunicerar som privatperson eller representerar Västerås stad. Läs mer om regler för sociala medier på Insidan.

Beställning av varor via Internet eller deltagande i chatsidor, anslagstavlor, bloggar, nyhetsgrupper, anmälan till mailinglistor eller liknande får bara göras i den mån det behövs i tjänsten.

Det är inte tillåtet att besöka webbplatser med extrempolitiskt eller pornografiskt innehåll, eller annat kränkande eller stötande material.

## 2.4. Lagring

Verksamhetsrelaterad information ska lagras på gemensamma diskutrymmen eller andra rekommenderade lagringsplatser. Mängden lagrad information ska av kostnadsskäl begränsas och information ska, om möjligt, inte lagras på flera ställen.https://insidan.vasteras.se/organisation/digitalisering/informationssakerhet/Sidor/Klassning-av-lös-information-och-filer.aspx

Verksamhetsrelaterad information bör inte enbart lagras lokalt på din dator, då denna inte säkerhetskopieras. Använd din hemkatalog!

Känslig eller sekretessbelagd information får endast, om det finns krypteringsskydd eller motsvarande skydd installerat, lagras på bärbar dator, läsplatta, telefon eller annan bärbar utrustning. I de fall erhållna bilagor i e-postmeddelanden bedöms innehålla känslig eller sekretessbelagd information ska dessa inte öppnas på oskyddad utrustning.

Det är inte tillåtet att lagra verksamhetskritisk, känslig eller sekretessbelagd information på lagringsplatser som inte kan kontrolleras av Västerås stad, till exempel Dropbox, privat Onedrive, Google drive eller motsvarande.
Känslig eller sekretessbelagd information måste vara krypterad om den ska lagras på extern lagringsmedia, till exempel USB-minnen. Dessa ska förvaras och hanteras på ett säkert sätt. Extern lagringsmedia som inte längre används skall förstöras enligt rutin för destruktion.

## 2.5. Antivirusprogram

På stadens datorer finns antivirusprogramvara. Programvaran får aldrig stängas av eller på annat sätt göras inaktiv. Vid misstanke om att datorn har virussmittats, kontakta omgående Service Desk.
All inkommande e-post har passerat ett virusskydd för att minimera risken att drabbas av virus eller annan skadlig kod. En antivirusprodukt kan inte skydda mot allt. Därför ska man vara försiktig när man får meddelanden från misstänkt avsändare. Bifogade filer ska endast öppnas om de kommer från en känd avsändare och en bilaga är förväntad.

## 2.6. E-post

Sekretessbelagd information eller känsliga personuppgifter får inte skickas via vanlig e-post. För överföring av sådana uppgifter krävs kryptering. Se Insidan (https://insidan.vasteras.se/organisation/digitalisering/Sidor/Användarmanual-Säkra-Meddelanden.aspx )

Verksamhetsrelaterad information får inte skickas vidare eller automatiskt vidarebefordras till privat e-post.

Västerås stads e-postadress bör inte användas för privata syften, anställda uppmanas att skapa ett e-postkonto hos en extern leverantör för sin privata e-post.

## 2.7. Skräppost (spam)

Inkommande e-post passerar genom ett spam-filter för att sortera bort skräppost. Allt kan dock inte tas bort eftersom staden då riskerar att radera e-post som är relevant och som kan vara att betrakta som allmän handling.

Misstänkt spam skickas automatiskt till respektive användares skräppostkorg alternativt markeras med […SPAM?...] i ärenderaden. Alla användare måste

regelbundet kontrollera om det har hamnat verksamhetsrelaterade meddelanden i skräpposten.

Användaren ska undvika att klicka på bifogade länkar till externa webbsidor, då dessa kan innehålla virus, skadlig kod eller gå till skadliga internetsidor.

## 2.8. Datakommunikation

IT-utrustning som är ansluten till Västerås stads interna nät kommunicerar med hög säkerhet. Vid kommunikation från annan plats, till exempel via trådlösa nät, som på hotell, hot spots, caféer etc., ska användaren vara medveten om att det alltid finns risk att kommunikationen kan avlyssnas. Vissa tjänster från staden kan nås med enkel inloggning över internet. Men de flesta tjänster förutsätter att din dator ansluter till Västerås stad via VPN-tjänst, en säker krypterad överföring upprättas då mellan din dator och stadens nätverk och tjänster.

Det är inte tillåtet att på egen hand installera trådlös accesspunkt eller annan kommunikationsutrustning i stadens IT-miljö för att på så sätt skapa alternativa vägar för datakommunikation.

Det är endast tillåtet att ansluta Västerås stads utrustning till stadens nätverksuttag.

## 2.9. Telefoner och surfplattor

Telefoner och surfplattor innehåller funktioner såsom e-post och internet för informationsinhämtning m.m.

De telefoner och surfplattor som Västerås stad tillhandahåller kommer att utrustas med en säkerhetsfunktion som gör det möjligt för staden att på distans kunna administrera utrustningen. Staden har möjlighet att radera applikationer ”appar” eller information i utrustningen om skadlig kod, virus eller annat som hotar stadens IT-säkerhet skulle upptäckas, eller begränsa viss standardfunktionalitet i telefonen.

Varje användare ansvarar för att skapa ett konto för administration av telefonen eller surfplattan hos respektive tillverkare (Apple, Google, etc.). Användaren uppmanas vara försiktig med vilka applikationer (”appar”) som laddas ner och installeras på telefonen eller surfplattan. Ladda endast ner från kända och välrenommerade bibliotek. Eventuella kostnader förenade med köp av ”appar” ska hantera av användaren privat. I de fall ”appar” införskaffas i tjänsten ska kostnaden hanteras som utlägg.

För telefoner och surfplattor gäller samma regler för lagring som för övrig utrustning, se avsnitt 2.4. Information som lagras i telefoner och surfplattor säkerhetskopieras inte av Västerås stad. Varje medarbetare får själv säkerhetskopiera bilder eller annan information.

Västerås stad förbehåller sig rätten att radera en telefon eller surfplatta som kommit bort eller om andra säkerhetsmässiga behov föreligger. Detta kan i undantagsfall ske utan att användaren meddelas.

Användaren får inte manipulera telefonens eller surfplattans operativsystem, eller på annat sätt stänga av eller förändra konfigurerade säkerhetsinställningar.
Om telefonen eller surfplattan behöver repareras eller av någon annan anledning lämnas till tredje part ska all information raderas innan den lämnas bort. Det ligger på användarens ansvar att detta sker.

Medarbetare uppmanas att använda telefonen med försiktighet när det gäller användande och kommunikation, tänk därför på följande generella råd:

• Undvik att öppna SMS/MMS från okända avsändare, undvik även att klicka på länkar som mottas via SMS/MMS. Avaktivera automatisk öppning av textmeddelanden.

• Undvik att exponera telefonnumret i sammanhang som inte är arbetsrelaterade. Lägg till exempel inte upp telefonnumret på sociala medier.

### 2.10. Användning av privat eller annan organisations utrustning

Anställda som tar med sig sin privata utrustning och använder den i arbetet ska vara medvetna om att även den användningen kommer att loggas och vid misstanke om brott så kan kontroller göras även i den utrustningen.

Detsamma gäller för konsulter och andra visstidsarbetande som har med sig utrustning och genomför arbete åt staden med egen utrustning.

Generellt så gäller att enbart utrustning som ägs av staden får kopplas in på stadens nätverk. Det undantag som finns är Arosnet där även privat utrustning, elevdatorer eller annan organisations utrustning kan användas för inloggning. Det finns dock restriktioner i vilka resurser som en sådan utrustning kan nå.

### 2.11. Användande av IT-utrustning i utlandet

Det är endast tillåtet att använda IT-utrustningen för data- och telekommunikation utanför Sveriges gränser om det krävs i tjänsten.

## 3. IT-säkerhetsrelaterade incidenter

### 3.1. Arbetsgivarens kontroll

Västerås stad har som arbetsgivare rätt att kontrollera att regler i lagstiftning eller organisationens riktlinjer följs. Utöver vad som tidigare angivits gäller detta även filer och annat material som finns lagrat i datorer och nätverk. Även särskild programvara som automatiskt granskar och reglerar kommunikation, lagring och användning kan komma att användas.

Västerås stad kan även komma att logga trafik och funktioner i telefoner och surfplattor samt granska och analysera dessa för att säkerställa driften av dem och deras säkerhetsnivå.

Loggningen omfattar uppgifter om användarnamn och de flesta åtgärder som varje enskild användare gör och har gjort och kan alltså spåras i efterhand.

Slumpvisa kontroller kan komma att genomföras. Kontroll av enskilda användare kan även inledas på förekommen anledning.
Arbetsgivaren kan i enskilda fall komma att kontrollera innehåll i e-postmeddelanden om det är nödvändigt till exempel för att:

- uppfylla myndighetens skyldigheter om allmänna handlingars offentlighet,
- vid fara för informationssäkerhet, till exempel vid virusangrepp, eller
- för att utreda och förhindra brott men då alltid i samarbete med rättsvårdande myndigheter

Beslut om sådan kontroll fattas av Säkerhetsdirektör och genomförs i samråd med medarbetarens närmaste chef.

Vid akuta situationer kan avsteg från denna rutin ske för att i stället hanteras via IT-incidentprocessen.

Samtliga kontroller ska vara beslutade av behörig person, samt dokumenterade.

## 3.2. Åtgärder vid överträdelse av reglerna

Om kontroll av loggar tyder på att riktlinjerna har överträtts kommer detta att utredas av arbetsgivaren för att bedöma om arbetsrättsliga eller andra åtgärder ska vidtas mot någon anställd. Om arbetsgivaren finner att någon anställd kan misstänkas för brottslig handling kommer detta komma att anmälas till polis för utredning.

VÄSTERÅS STAD

Kontaktcenter: 021-39 00 00

www.vasteras.se