



# Datainstruks for Agder fylkeskommune

<b>Versjon/dato:</b> 03.01.2022	<b>Godkjent/vedtatt av:</b> Avdelingsleder for jus og informasjonsforvaltning
<b>Dokumentnummer:</b> 21/22666-1	<b>Beskrivelse:</b> Datainstruks for Agder fylkeskommune
<b>Neste versjon:</b> Skriv versjon	<b>Ansvar for revisjon:</b> Avdeling for jus og informasjonsforvaltning
<b>Første gang vedtatt:</b> 03.01.2022	<b>Gjelder for:</b> Alle ansatte i Agder fylkeskommune

## Innhold

1. Formål og innhold .....	2
2. Bruker ID – passord .....	2
3. Lås skjerm .....	2
4. Bærbare pc-er – oppdateringer .....	2
5. Sikkerhetstiltak .....	2
6. Privat bruk av fylkeskommunens utstyr .....	3
7. Bruk av privat datamaskin .....	3
8. Lagring av – og tilgang til data .....	3
9. Særlig om e-post .....	4
10. Installasjon av utstyr og programvare på fylkeskommunens datamaskin mobiltelefon og annet portabelt utstyr .....	4
11. Bruk av datautstyr utenfor fylkeskommunens nettverk .....	4
12. Internettbruk .....	5
13. Innlevering ved avsluttet arbeidsforhold .....	5
14. Rapportering og avvik .....	5

## 1. Formål og innhold

Formålet er å tilrettelegge for god, sikker og lovlig bruk av fylkeskommunens dataverktøy og systemer

## 2. Bruker ID – passord

Hver bruker har en personlig identifikasjon gjennom eget brukernavn og passord. Passord er strengt personlig og skal ikke oppgis til eller lånes ut til andre. Dette er et personlig ansvar.

Valgt passord skal være lett å huske, men det skal ikke inneholde navn på familiemedlemmer, fødselsnummer eller andre opplysninger som lett lar seg knytte til brukeren.

Passordet skal bestå av en kombinasjon av store og små bokstaver og tall/tegn og være på minst 8 tegn. Siste 5 passord skal ikke gjenbrukes.

Dersom du har mistanke om at passordet har blitt kjent av uvedkommende, skal passordet byttes og hendelsen rapporteres som avvik i QM+.

## 3. Lås skjerm

For å hindre at uvedkommende /andre får tilgang til din datamaskin når du selv ikke bruker den/ ikke er på arbeidsplassen, skal maskinen enten slås av eller skjermen låses.

## 4. Bærbare pc-er – oppdateringer

Alle som har bærbar pc må jevnlig – og minst en gang pr. måned - logge maskinen på fylkeskommunens nettverk slik at nødvendige oppdateringer av programvare kan finne sted.

## 5. Sikkerhetstiltak

Alle ansatte er forpliktet til å følge de retningslinjer for IKT-sikkerhet fylkeskommunen iverksetter.

Lagringsmedier som inneholder personopplysninger/taushetsbelagte opplysninger skal håndteres og oppbevares på en måte som gjør at opplysningene ikke kommer på avveie. Papirutskrifter som inneholder personopplysninger den ansatte ikke lenger har behov for skal makuleres.

Se rutine for [Digital lagring i Agder fylkeskommune](#) og rutine for grunnlagsdokumentasjon for sikkerhetsdokumentasjon (under utarbeidelse) i QM+.

Personopplysninger skal kun lagres i systemer som er beregnet for dette formålet.

Ettersom nøkkel/nøkkelkort er et sentralt punkt for å skjerme informasjon så må medarbeidere umiddelbart melde fra til arbeidsgiver ved tap av disse.

Den som mottar besøkende, er ansvarlig for at gjesten ikke får tilgang til konfidensiell informasjon

## 6. Privat bruk av fylkeskommunens utstyr

Agder fylkeskommunens datautstyr er stilt til disposisjon for bruk som arbeidsverktøy. Den enkelte ansatte kan bare bruke dette til private oppgaver i begrenset omfang. All privat bruk skal skje innenfor denne instruksjonen. Det er ikke adgang til å låne fylkeskommunens datautstyr til andre familiemedlemmer eller uvedkommende. Det er heller ikke adgang til å bruke fylkeskommunens datautstyr i egen næringsvirksomhet. Fylkeskommunen fraskriver seg alt ansvar for tap av private data, ved uhell eller vedlikehold/service på maskin/server/enheter.

Fylkeskommunens datautstyr skal ikke brukes til å lagre eller spre materiale som er diskriminerende, pornografisk eller på annen måte fremstår som støtende.

## 7. Bruk av privat datamaskin

Informasjon knyttet til fylkeskommunen eller fylkeskommunens innbyggere/leverandører/ansatte/ samarbeidspartnere osv. tillates ikke lagret på privat datamaskin eller i privat e-postkontoer.

## 8. Lagring av – og tilgang til data

Som hovedregel skal alle data lagres i fylkeskommunens sak- og arkivsystem eller de fagsystemer saken hører hjemme i. Beskyttelsesverdig informasjon skal ikke lagres på bærbar PC, telefoner eller annet portabelt utstyr med mindre det er installert godkjente sikkerhetsløsninger (normalt med kryptert disk).

Lagring av andre fylkeskommunale data og arbeidsdokumenter skal skje i henhold til gjeldende retningslinjer for [Digital lagring i Agder fylkeskommune](#), som ligger i QM+.

Den ansatte skal foreta fortløpende rydding på sine områder.

Personopplysninger og annen beskyttelsesverdig informasjon som behandles skal være beskyttet mot uautorisert tilgang.

Data som inneholder personopplysninger skal lagres slik at de kun er tilgjengelig for medarbeidere som har behov for opplysningene i sitt arbeid. Alle data som inneholder helseopplysninger skal kun lagres i definerte fagapplikasjoner eller sak og arkiv system med riktig skjerming. Dersom du trenger hjelp med å finne riktig skjermingsbestemmelse ta kontakt med avdeling for jus og informasjonsforvaltning.

Agder fylkeskommune har i utgangspunktet ikke adgang til å gå inn på den enkelte ansattes personlige område og e-postboks. Innsyn i ansattes personlige områder og e-postboks må følge forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale.

Det vises til rutinen for behandling av personopplysninger punkt. 11 for ytterligere presisering av arbeidsgivers innsyn i e-poster og elektroniske filer.

## 9. Særlig om e-post

Fylkeskommunens e-post er opprettet som et arbeidsverktøy. All e-post som benyttes i arbeidet skal skje gjennom fylkeskommunens e-postløsning. Systemet tillates i begrenset grad brukt til private formål.

E-postsystemet skal ikke brukes til å spre materiale som er diskriminerende, pornografisk eller på annen måte fremstår som støtende eller plagende.

E-postsystemet er ikke et saksbehandlerprogram. E-post som inngår som del av saksbehandlingen skal legges inn i vedkommende saksbehandlersystem. Brukere er selv ansvarlig for å vurdere hva som er arkivverdig.

Oversikt over hva som kan være arkivverdig finner du [her](#).

Utover det angitte foran gjelder følgende regler ved bruk av e-post:

- E-post skal ikke brukes når det er konfidensiell eller sensitiv informasjon uten at innholdet er kryptert eller anonymisert. Ved forsendelse av personopplysninger gjelder personopplysningsloven. En huskeregel er å vurdere hvilke konsekvenser en feilsending kan få.
- Dersom en ansatt er forhindret fra å lese e-post i flere arbeidsdager bør fraværsassistenten / automatiske svar brukes.
- Kjedebrev eller lignende tillates ikke videresendt eller distribuert.

Se også [Regler for sending av epost i QM+](#)

Når arbeidstaker slutter blir vedkommendes epostkasse avsluttet. Den ansatte har ansvar for at all arkivverdig materialer som ligger på eposten blir arkivert før arbeidsforholdet avsluttes.

## 10. Installasjon av utstyr og programvare på fylkeskommunens datamaskin mobiltelefon og annet portabelt utstyr

PC, mobiltelefon og annet portabelt utstyr som er gjort tilgjengelig i jobb, er i utgangspunktet konfigurert av IKT Agder. Dette oppsettet skal ikke endres av bruker.

Enhver installasjon utover det som utgjør fylkeskommunens IT-plattform skal være faglig begrunnet, og ved tvil skal informasjonssikkerhetsansvarlig godkjenne installasjonen. Den ansatte er selv ansvarlig for konsekvensene ved egen installasjon. Ved egen installasjon forutsettes at det foreligger brukerlisens. Kopiering av lisensiert programvare er forbudt.

Agder fylkeskommune kan uten varsel fjerne programvare som er lagt inn i strid med foranstående, eller programvare som ikke følger norsk lov. Det er ikke tillatt å koble privat eller fremmed IT-utstyr opp mot fylkeskommunes kablede nettverk uten skriftlig godkjenning fra informasjonssikkerhetsansvarlig.

## 11. Bruk av datautstyr utenfor fylkeskommunens nettverk

Ved oppkobling av fylkeskommunale PC-er og andre digitale enheter, mot eksterne datanettverk må brukeren utvise særskilt aktsomhet. På reise skal mobilt bredbånd benyttes fremfor gratis offentlige nettverk (free wifi).

Dersom ansatte skal medbringe slikt utstyr til land som kan utgjøre en sikkerhetsrisiko, må dette avklares med sikkerhetsansvarlig.

## 12. Internettbruk

Det er ikke tillatt å laste ned utuktig materiale, opphavsrettslig beskyttet materiale (f.eks. musikk, filmer og programvare) eller annet som er i strid med lovverket på utstyr som arbeidstakeren har fått tilgjengeliggjort av arbeidsgiver eller via kommunens nettverk.

Ved bruk av Internett opptre man som en representant for fylkeskommunen. De samme retningslinjer som ved all annen kontakt på vegne av fylkeskommunen gjelder. Informasjon som av medier eller opinion oppfattes som pornografisk, rasistisk, kriminell eller av uetisk natur, skal derfor ikke oppsøkes, kopieres eller lastes ned til it-utstyr som eies eller driftes av fylkeskommunen.

Fylkeskommunen har anledning til å logge informasjon om Internett og e-post trafikk for å sikre alminnelig drift, samt for sporing ved eventuelle sikkerhetsbrudd.

## 13. Innlevering ved avsluttet arbeidsforhold

Ansatte som har bærbar PC, iPad, mobiltelefon eller annet utstyr skal ved avslutning av arbeidsforholdet innlevere dette utstyret senest siste arbeidsdag. Dersom det er inngått avtale om overtagelse av deler av dette utstyret, kan den ansatte kjøpe ut dette utstyret etter satsene i [Agder fylkeskommunes økonomireglementet](#) punkt. 10.1, som ligger i QM+.

Dersom utstyr er avtalt medtatt, skal dette leveres inn slik at data/informasjon som er relatert til vedkommendes arbeid fjernes. Det er ikke tillatt å kopiere/medbringe lagret informasjon, som er relatert til vedkommendes arbeid.

Utstyr som den ansatte har som er på leasing avtale kan ikke den ansatte overta.

Autorisasjoner for fjerntilgang, skal leveres tilbake senest siste arbeidsdag.

Annet tidspunkt enn nevnt over kan avtales mellom arbeidsgiver og arbeidstaker.

## 14. Rapportering og avvik

Dersom det oppdages sikkerhetsbrudd eller hendelser som kan ha betydning for sikkerheten skal fylkeskommunens avvikshåndteringssystem benyttes i QM+.

### [Avvik – informasjonssikkerhet og personvern](#)

Avhengig av type hendelse og tidsperspektiv må det meldes fra til nærmeste leder og systemansvarlig. Se også rutine for behandling av personopplysninger i QM+.

Dersom det oppdages virus eller annen skadelig programvare, dataangrep eller annet unormal aktivitet på datautstyr eller telefoner, skal nærmeste leder og IKT Agder varsles umiddelbart.

[Oversikt over systemansvarlige](#) som ligger i QM+.