



## Innledning

Informasjons- og kommunikasjonsteknologi gir deg viktige verktøy for deg som ansatt i Finnmark fylkeskommune (heretter: FFK), og skal muliggjøre og hjelpe deg å utføre dine arbeidsoppgaver best mulig. Som ansatt vil du få tilgang til ressurser, informasjon og systemer etter hvilke funksjoner og oppgaver du skal utføre.

Dette reglementet skal ivareta informasjonssikkerheten, forhindre misbruk eller ulovlig bruk av ressurser, informasjon og systemer, samt bidra til merverdi for deg i arbeidet ditt.

## Virkeområde

Reglementet regulerer rettigheter og plikter ved bruk og tilgang til FFKs IT-ressurser, inkludert datanettverk, informasjon, maskinvare og programvare anskaffet eller disponert av FFK (heretter: IT-infrastruktur). Reglementet gjelder alle som har tilgang til FFKs infrastruktur, inkludert ansatte, politikere, elever og eventuelt andre som får utstyr eller tilgang til FFKs IT-ressurser.

Reglementet skal være lest og akseptert før tildeling av brukerkonto.

Skolene kan ha egne utfyllende regler, som ikke må være i strid med dette IKT-reglementet.

## Generelle bestemmelser

All IKT-infrastruktur skal anses som FFKs eiendom. Denne infrastrukturen skal benyttes til formålstjenlige aktiviteter i tilknytning til arbeidet ditt. Selv om en rekke sikkerhetstiltak er iverksatt for å beskytte mot ondsinnet programvare og andre trusler mot informasjonssikkerheten, er alle brukere ansvarlige for å benytte infrastrukturen på en profesjonell, lovlig og etisk forsvarlig måte.

## Brukerkonto

Din brukerkonto, med tilhørende brukeridentifikasjon og passord er personlig.

- Ikke oppgi passord eller andre tilgangsnøkler til andre.
- Ikke la andre bruke utstyr der du er allerede innlogget uten din tillatelse.
- Forlates utstyr der du er innlogget må dette sikres med skjermlås.

## Bruk av nettverk

### Generelt

Nettverksbåndbredde og tilhørende ressurser er begrensede, og alle brukere er ansvarlige for å ikke med overlegg bruke disse ressursene på en slik måte at andre ikke får tilgang. Dette inkluderer, men er ikke begrenset til, masseutsendelse av e-post, dataspill, deltagelse i



diskusjonsgrupper, opp- eller nedlasting av store filer eller annen aktivitet som medfører høy nettverksbelastning.

Ved mistanke om misbruk kan utstyr bli frakoblet nettverksressurser uten forvarsel.

FFK har rutiner for å hindre spredning av ondsinnet programvare og andre trusler. Dette fritar ikke den enkelte bruker i å utvise forsiktighet for å hindre at slike trusler får tilgang til IKT-infrastrukturen. Filer mottatt fra kilder utenfor FFK, inkludert, men ikke begrenset til, filer lastet ned fra Internett, inkludert e-post og tilkoblede media kan inneholde skadelige filer. Dersom du mistenker at virus eller lignende trusler har blitt introdusert til IT-infrastrukturen, plikter du gjøre nærmeste leder eller systemansvarlig oppmerksom på dette.

Vær oppmerksom på at taushetsbelagt materiale på elektronisk form behandles på samme måte som annet taushetsbelagt materiale. Materiale som er taushetsbelagt, sensitivt, eller på annen måte unntatt offentlighet skal ikke publiseres eller distribueres med mindre eksplisitt dispensasjon har blitt gitt.

## **Internett**

For å opprettholde sikkerheten og unngå spredning av ondsinnet programvare, skal brukere kun koble seg til Internett via FFKs brannmurer. Det er ikke tillatt å omgå disse sikkerhetsløsningene. Dette inkluderer tilkobling direkte til modem eller andre kommunikasjonsløsninger. Bruk av trådløse rutere på arbeidsstedets område er ikke tillatt da dette kan hindre eller forstyrre effektiv bruk av FFKs eget datanettverk.

- Brukere skal ikke oppsøke, overføre eller lagre innhold fra kilder der du er, eller burde vært, kjent med som inneholder pornografisk, rasistisk eller annet lovstridig og / eller uetisk innhold. I den grad slikt innhold skulle være nødvendig som ledd i saksbehandling, må tillatelse fra nærmeste leder være innhentet.
- Trusler, mobbing eller andre krenkelser via digitale kanaler er ikke tillatt.
- Du må innhente samtykke fra berørte parter før bilder eller videoer med identifiserbare personer blir tilgjengeliggjort. Dette gjelder også kanaler med begrenset tilgjengelighet.
- Du bruker Internett på eget ansvar, og FFK er ikke ansvarlig for materiale som oppsøkes eller lagres av den enkelte bruker.

## **E-post**

- Sensitive personopplysninger skal ikke sendes via e-post. Mottas e-post med slikt innhold, skal den ikke videresendes, besvares eller kommenteres.
- Brukere skal ikke sende eller videresende e-post med lovstridig eller uetisk innhold.
- Vær oppmerksom på e-poster med filvedlegg, og unngå å åpne vedlegg som kommer fra en ukjent kilde eller som du mistenker kan inneholde ondsinnet programvare.
- Vær oppmerksom på e-poster som ber om innloggingsdetaljer eller annen personlig informasjon.

Hver bruker representerer FFK ved bruk av Internett og når du kommuniserer med andre via FFKs infrastruktur. Private ytringer skal ikke assosieres med fylkeskommunen.



## Programvare

Du skal ikke installere programvare uten skriftlig tillatelse fra FFK. Bruker skal ikke distribuere eller tilgjengeliggjøre kopier av kopibeskyttet materiale, og er selv ansvarlig for å overholde andre bestemmelser om kopibeskyttelse. Programvare, innstillinger og annen funksjonalitet som er installert av IT-ansvarlig må ikke endres, fjernes eller erstattes.

## Personlig data

FFK har ikke ansvar for lokal data som går tapt som følge av skade på eller feil bruk av IKT-utstyr. Brukere må selv sørge for sikkerhetskopier av slik data. Ved opphør av arbeidsforhold er brukere selv ansvarlig for kopier av personlige data.

## Overvåking og innsyn

FFK kan overvåke bruk av IT-infrastrukturen og føre logg over dette. Formålet er ikke individuell overvåking, men et sikkerhetstiltak for å beskytte infrastrukturen mot trusler og misbruk. FFK kan blokkere tilgang til Internettressurser som inneholder upassende materiale.

Ved brudd, eller mistanke om brudd, på IKT-reglementet kan disse loggene benyttes som grunnlag for videre vurdering av eventuelt brudd.

All databasert overvåking av bruk av IKT-infrastruktur i FFK skjer i henhold til Datatilsynets pålegg og retningslinjer. FFK forbeholder seg retten til innsyn i arbeidstakers epost og andre filer, som regulert i «[Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale](#)»

## Varsling

Sikkerhetsbrudd skal rapporteres til nærmeste overordnede som er ansvarlig for viderebehandling.

## Sanksjoner ved brudd

Misbruk av IKT-infrastrukturen kan føre til disiplinære forføyninger, herunder tap av rett til bruk av ressursene. Disiplinære forføyninger vil her bety det samme som ved brudd på andre arbeidsavtaler og etiske reglement. Bruker kan også bli pålagt erstatnings- og straffeansvar.

Du må alltid vise skjønn i forhold som ikke direkte er adressert i retningslinjene og som kan påføre FFK skade.