Informasjonssikkerhet

Brukerinstruks

for

ANSATTE I

RANA KOMMUNE

Versjon 2.2011

INNHOLD

DEL 1- DEFINISJONER

1.1. DEFINISJONER (POL § 2)

A. PERSONREGISTER:

registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen.

B. PERSONOPPLYSNINGER:

opplysninger og vurderinger som kan knyttes til en enkeltperson

C. BEHANDLING AV PERSONOPPLYSNINGER:

enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

D. REGISTRERT:

den som en personopplysning kan knyttes til.

E. SAMTYKKE:

en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv.

F. SENSITIVE PERSONOPPLYSNINGER:

Opplysninger om:

- rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning.
- at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
- helseforhold
- seksuelle forhold
- medlemskap i fagforeninger

G. BEHANDLINGSANSVARLIG/DATABEHANDLER

Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Databehandler behandler personopplysninger på vegne av den behandlingsansvarlige.

1.2. INNLEDNING

Kommunens rolle i samfunnet innebærer en naturlig forpliktelse til å holde et høyt etisk nivå og sikre riktig kvalitet på sine primæroppgaver. Kommunens drift og organisering medfører at sensitiv opplysninger behandles i mange ledd. Myndighetene har derfor fastsatt et regelverk for kontroll og sikkerhet som krever systematisk oppfølging.

De overordnede mål for informasjonssikkerhetsarbeidet for Rana kommune er å oppnå høy grad av:

- Tilgjengelighet – er det tilgjengelig når du trenger det
- Konfidensialitet – opplysninger skal ikke eksponeres for uvedkommende
- Integritet – sikre informasjon mot utilsiktet endring

Det betyr at de data som vi registrerer i våre datasystemer skal være korrekte, de skal være tilgjengelige når det er behov for dem og de skal være beskyttet mot uvedkommende.

1.3. ANSVAR OG MYNDIGHET

Rådmannen har det overordnede ansvaret for at behandling av personopplysninger i kommunen, er i samsvar med personopplysningsloven (POL). Produksjonssjefene er behandlingsansvarlig i sin avdeling. Rollen som behandlingsansvarlig kan delegeres i linja.

Hun/han er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler, herunder systemer og rutiner/prosedyrer som skal etableres og brukes (ref. pol § 2 pkt. 4) for å oppfylle de aktuelle lovkrav.

Den enkelte saksbehandler som behandler personopplysninger på oppdrag fra behandlingsansvarlig , er databehandler (ref. pol. § 2 pkt. 5). Hun/han er ansvarlig for å sette seg inn i og behandle opplysningene i samsvar med gjeldende lovverk og de rutiner produksjonssjef/ behandlingsansvarlig har godkjent.

Lærlinger, elever og studenter i praksis er ansvarlig for å sette seg inn i avdelingens rutiner for behandling av personopplysninger. Studentens behandling av personopplysninger skal kun skje i opplæringsøyemed og under veiledning av dataansvarlig saksbehandler eller behandlingsansvarlig som behandlingsansvarlig.

Forholdet mellom personopplysningsloven og særlovgivning på tjenesteområdene:

Der det i særlovgivning stilles skjerpede krav til behandling av personopplysninger, skal behandlingsansvarlig sikre at det etableres rutiner som ivaretar disse kravene.

Alle som utfører arbeid for kommunen, ansatte, midlertidig ansatte og oppdragstakere har lovbestemt taushetsplikt. Plikten gjelder både i arbeidet og privat, og den varer også etter avsluttet arbeidsforhold i kommunen.

Lederen for den enkelte avdeling/enhet/kontor har ansvar for å opprettholde en tilfredsstillende informasjonssikkerhet innenfor sitt ansvarsområde.

Den enkelte medarbeider har ansvar for å sette seg inn i informasjonssikkerhets-linjene og følge disse.

God informasjonssikkerhet oppnås gjennom den enkelte ansattes holdning og årvåkenhet, og ved at den enkelte ansatte kan vise ansvar for informasjons- sikkerheten og følge gjeldende retningslinjer innenfor sitt arbeidsområde.

1.4. EGENERKLÆRING –BRUDD PÅ RETNINGSLINJENE.

Ansatte, konsulenter og vikarer etc. skal rette seg etter sikkerhetsinstruksen (dette dokumentet) og underskrive standardisert egen erklæring, samt taushetserklæring. I egenerklæringen bekreftes det at man har lest og signert sikkerhetsinstruksen som gjelder for Rana kommune. Signert egenerklæring og taushetserklæring for ansatte skal oppbevares i personalmappen.

Konsekvenser for ansatte som har forårsaket brudd på sikkerhetsreglene , vil bli vurdert i hvert enkelt tilfelle og kan ved alvorlige brudd føre til oppsigelse/avskjed (jfr. virksomhetens reglement/ Lovverk).

1.5. INNLEID PERSONELL

Innleid personell skal behandles som besøkende og hentes og følges under arbeidet spesielt i områder hvor sensitiv informasjon eksponeres, med mindre den behandlingsansvarlig som har ansvaret for arbeidet gir dispensasjon. Ikke under noen omstendighet skal teknikere og andre eksterne fritt kunne oppholde seg inne på maskinrom (tekniske rom, datarom, osv.), dvs de skal alltid ha følge av fast ansatt personell. (Unntaket er autorisert personell som har underskrevet taushetsløfte).

1.6. AVVIKSBEHANDLING

POF § 2-6 Avvik
Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik.

Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse. Dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles. Resultatet fra avviksbehandling skal dokumenteres.

Avvik fra denne instruks skal håndteres som avvik og varsles umiddelbart.. Avviksmeldingen skal leveres behandlingsansvarlig og kopi sendes sikkerhetsansvarlig i Rana kommune.

1.7. SIKKERHET OG ORDEN PÅ KONTORET

- La ikke sensitiv/fortrolig informasjon ligge å flyte på skrivebordet, skrivere etc.
- Kast ikke sensitive/fortrolige dokumenter, usb- penner, CD'er etc. i papirkurven. Makuler dem!
- Uvedkommende skal ikke ha tilgang til steder hvor datautstyr, skrivere, kommunikasjonsutstyr, telefakser o.l. er plassert, uten i følge med ansatt
- Den enkelte medarbeider skal aktivt bidra til at det ikke blir liggende igjen personopplysninger på skrivere og kopimaskiner som eksponeres for uvedkommende.

DEL 2. INFORMASJONSSIKKERHETSINSTRUKS FOR ANSATTE I RANA KOMMUNE.

2.1. BRUKER ID – PASSORD

For å få tilgang til kommunens datasystemer, må alle ansatte, oppdragstakere og midlertidige ansatte gis nødvendige autorisasjoner gjennom sin leder, og taushets- og arbeidsavtale må undertegnes. Nødvendige opplæringstiltak skal være gjennomgått.

Hver bruker har en personlig identifikasjon gjennom eget brukernavn og passord. Det skal velges passord som ikke lett lar seg knekke av uvedkommende. Passordet skal ikke meddeles andre uten at arbeidsgiver (nærmeste leder) har samtykket (straffelovens § 145b). Den enkelte ansatte er selv ansvarlig for de handlinger som utføres med egen identitet. Du må straks endre passord hvis det har blitt kjent av andre.

2.1. LOGG UT/ SLÅ AV

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 sperres ved Windows tasten + L eller Ctrl + alt + delete og trykk på Lås datamaskinen.

For å unngå misbruk, men også av hensyn til brannfare skal maskinen fysisk slås av ved arbeidstidens slutt. På arbeidsplasser med åpne kontorløsninger skal den enkelte ved fravær over 10-15 minutter (helst når arbeidsplassen forlates for mer enn et kort ærend) sperre tilgangen via Windows tasten + L. For de med egne kontorer kan et alternativ være å låse døren ved fravær.

2.2. BÆRBARE PC-ER.

Det er ikke anledning til å lagre sensitive personopplysninger på bærbare maskiner med mindre spesiell tillatelse er gitt av behandlingsansvarlig i samråd med sikkerhetsansvarlig.

Alle som har bærbar pc må jevnlig – og minst en gang pr. måned - logge maskinen på kommunens nettverk for å oppdatere antivirusprogram. Den som disponerer bærbar pc skal ikke fjerne eller deaktivere antivirusprogramvare som er installert på pc-en. Oppdateringen skjer automatisk.

Det er ikke anledning til å koble opp private pcèr mot det kommunale nettverket. Unntak er møterom på Rådhuset fordi det her er ren Internett aksess.

Har den ansatte mistanke om at det kan være virus eller annen skadelig programvare på utstyret, skal den ansatte straks levere datamaskinen til IKT-avdelingen. Maskinen skal ikke kobles inn i kommunens nett.

2.3. SIKKERHETSTILTAK

Alle ansatte er forpliktet til å følge de sikkerhetstiltak arbeidsgiver iverksetter. Lagringsmedier (disketter, USB (penn/minne/disk), CD-plater, tape og papirdokumenter) som inneholder personopplysninger/ taushetsbelagte opplysninger skal håndteres og oppbevares på en måte som gjør at opplysningene ikke kommer på avveie. Slike lagringsmedia skal ikke tas ut av kommunens lokaler og skal låses ned når de ikke er i bruk.

Lagringsmedia og papirutskrifter som inneholder personopplysninger den ansatte/virksomheten ikke lenger har behov for skal makuleres på en forsvarlig måte. Arkivloven med kassasjonsbestemmelser.

Rutine for informasjonshåndtering som inngår som en del av sikkerhets instruksen skal følges ved håndtering av informasjonsflyt i Rana kommune – se Vedlegg 1.

2.4. PRIVAT BRUK AV ARBEIDSGIVERS UTSTYR

Arbeidsgivers 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 instruksen. Det er ikke adgang til å låne kommunens datautstyr til uvedkommende. Det er heller ikke adgang til å bruke kommunens datautstyr i egen næringsvirksomhet uten etter skriftlig avtale med rådmannen eller den han/hun utpeker.

2.5. NEDLASTING AV FILER SOM TAR STOR KAPASITET

Nedlasting / lagring av filer over kommunens nett er ikke tillatt, f.eks. bilder, film og musikkfiler, er kun tillatt såfremt dette er helt nødvendig i jobbutførelsen. Ved behov eller tvil skal nærmeste leder forespørres/ varsles. I den grad det ikke er påkrevd av hensyn til jobbutførelse må samme fil ikke lagres flere steder.

2.6. LAGRING AV – OG TILGANG TIL DATA

Lagring av kommunale data skal skje på fellesområder etter anvisning bestemt av den enkelte virksomhet. Som utgangspunkt skal alle data lagres i saksbehandlerprogram saken hører hjemme i, primært EDB sak/arkiv eller tilhørende fagsystem som er i drift

Ikke-arkivverdige dokumenter som er felles for hele kommunen skal lagres på F-området (fellesområde for tilhørende enhet) og H-området (ansattes eget område) i anvist mappe.

Private dokument, (jfr. pkt. 2.6 foran om at dette er tillat i begrenset omfang) lagres på ansattes H -område.

Den ansatte skal foreta løpende rydding på sine områder, og skal ikke lagre filer som bilder/program/video eller andre data, såfremt dette ikke er helt nødvendig i jobbutførelsen. (link til innsia IKT brukerstøtte)

Arbeidsgiver har full tilgang til alle dokumenter/ alle filer som er lagret på fellesområdene.

Arbeidsgiver har i utgangspunktet ikke adgang til å gå inn på den enkelte ansattes H-området. Blir arbeidsgiver oppmerksom på at det er stor sannsynlighet for at det lagres arbeidsrelaterte dokumenter (f.eks. arkivverdige dokumenter) på H-området, lokale disker eller andre lagringsenheter kan arbeidsgiver gi en kort frist for å rette opp i tråd med instruksen. Det samme gjelder hvis arbeidsgiver har mistanke om at det lagres ting som ikke er nødvendig i jobbutførelsen.

Hvis opprydding ikke er foretatt innen fastsatt frist kan arbeidsgiver gå inn og overføre arkivverdige dokumenter til riktig saksbehandlersystem og/eller slette data som ikke er nødvendig i jobbutførelsen. Det samme gjelder hvis det er begrunnet mistanke om praktisering i strid med gjeldende retningslinjer eller norsk lov, eller det lagres filer som tar stor plass/ kapasitet, se punkt foran, eller lagring av ulovlig materiale.

Ved åpning av H-området i henhold til avsnittet foran skal to personer fra arbeidsgiver og en representant for vedkommende ansatte (tillitsvalgte eller verneombud) være til stede. Det utarbeides protokoll som sendes den ansatte. Det skal ikke åpnes dokumenter i større utstrekning enn nødvendig for å ivareta formålet med innsynet.

2.7. SÆRLIG OM E-POST (SE OGSÅ VEDLEGG 2)

Arbeidsgivers e-post (Microsoft Exchange) er opprettet som et arbeidsverktøy. E-post må som annen post håndteres i samsvar med forvaltningsloven offentlighetsloven, personopplysningsloven, god forvaltningsskikk og andre forvaltningsrettslige prinsipper og regelverk. Rana kommune har utarbeidet retningslinjer for behandling av e-post som alle ansatte er forpliktet til å sette seg inn og etterleve. Se vedlegg 2.

Presiseringer i tillegg til gjeldende retningslinjer:

- E-postsystemet skal ikke brukes til å spre materiale som er diskriminerende, pornografisk eller på andre måter fremstår som støtende.
- E-postsystemet er ikke et saksbehandlerprogram. E-post som inngår som del av saksbehandlingen skal videresendes postmottaket, eller oversendes arkiv for skanning og tilknytting til den aktuelle saken.
- Det er ikke adgang til å gi andre brukertilgang til egen e-postkonto.
- Arbeidsgiver skal i utgangspunktet ikke gå inn i den enkelte ansattes e-postsystem uten samtykke fra den ansatte.
- For å sikre tilgang til arbeidsrelatert e-post kan arbeidsgiver – om nødvendig – gå inn i den enkeltes e-postsystem ved fratredelse av stilling og i tilfeller der den ansatte har lengre fravær og det er vanskelig å få kontakt. Det vises i den sammenheng til bruk av fraværsagent , se under. Det samme gjelder hvis det er begrunnet mistanke om at det praktiseres i strid med gjeldende retningslinjer eller norsk lov, eller det lagres filer som tar stor plass/ kapasitet – se punktet foran – eller det lagres ulovlig materiale. Før eventuell åpning skal det vurderes om det er andre muligheter til å innhente opplysning ene på. Tillitsvalgt og / eller verneombud skal rådføres.
- Den ansatte skal foreta løpende rydding på sitt e-postområde. Uavhengig av det som er bestemt i avsnittet foran kan arbeidsgiver uanmeldt gå inn når dette er nødvendig av administrative årsaker, eks. virusangrep. Den/ de ansatte skal i ettertid ha generell informasjon om dette. Samme informasjon skal gå til de tillitsvalgte.
- Det er taushetsplikt på private opplysninger man blir kjent med ved innsyn.
- Utover det angitte foran gjelder følgende regler ved bruk av e-post: E-post skal ikke brukes når det gis konfidensiell eller sensitiv informasjon uten at innholdet er kryptert eller anonymisert. Ved forsendelse av personopplysninger gjelder personopplysningsloven.
- Ved lengre fravær (over 3 arbeidsdager) **SKAL** fraværsagenten brukes (jfr. pkt. 10-retningslinjer).
- Kjedebrev eller lignende tillates ikke videresendt eller distribuert.
- Intern post til ”Alle” er ikke tillatt uten særskilt godkjenning. Det skal for øvrig vises stor varsomhet med å sende e-post som masseutsendelser.
- Tillitsvalgte og vernetjenesten skal ha egne e-postadresser som arbeidsgiver ikke kan åpne uten samtykke.

2.8. “SNOKING” I JOURNALER

Fra 9. mai 2009 er det straffbart ”å snoke” i journaler. Hittil har snoking bare vært underlagt tjenstlige reaksjoner. Nå risikerer ansatte som bryter med brudd på reglene om snikkikking

opptil 3 måneders fengsel. Alle ansatte med tilgang til pasientopplysninger må derfor være om mulig enda mer bevisst på at snoking ikke kan tolereres.

Helseregisterloven lyder:
§ 13a. *Forbud mot urettmessig tilegnelse av helseopplysninger*
Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger som behandles etter denne loven uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.

§ 34. *Straff*
Den som forsettlig eller grovt uaktsomt overtrer § 13 a, straffes med bøter eller fengsel i inntil tre måneder.

Helsepersonelloven:
§ 21a. *Forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger*:
Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte opplysninger som nevnt i § 21 uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.

§ 67. *Straff*
Den som forsettlig eller grovt uaktsomt overtrer eller medvirker til overtredelse av bestemmelser i loven eller i medhold av den, straffes med bøter eller fengsel i inntil tre måneder. Offentlig påtale finner sted hvis allmenne hensyn krever det eller etter begjæring fra Statens helsetilsyn.

2.9. TELEFAKS/SKRIVER

Sensitive opplysninger skal ikke sendes via telefaks. Telefaks må som annen post håndteres i samsvar med forvaltningsloven offentlighetsloven, god forvaltningsskikk og andre forvaltningsrettslige prinsipper og regelverk.

Telefaks som inngår som del av saksbehandlingen skal videresendes postmottaket, eller oversendes arkiv for skanning og tilknytting til den aktuelle saken. Det anbefales at alle inn komne telefakser rutes mot kommunens offisielle e-postadresse postmottak@rana.kommune.no for å sikre korrekt håndtering.

Når man benytter utskrift skal man alltid velge fil – skriv ut og velge rett skriver. Dette for å forhindre valg av feil skriver. Ved utskrift av konfidensielle opplysninger skal det alltid velges utskrift med pinkode. Hvis man har en eldre skriver som ikke støtter slik utskrift skal utskriften hentes straks den blir printet ut.

Det vises til vedlegg 1. Rutine for informasjonshåndtering som er en del av denne instruksen..

2.10. INSTALLASJON AV UTSTYR OG PROGRAMVARE PÅ EGEN MASKIN.

Kun programvare som er lisensiert til kommunen og som IKT –avdelingen har godkjent kan benyttes på kommunens pc èr og nettverk. Kopiering av kommunens programvare uten tillatelse er forbudt.

Enhver installasjon utover det som utgjør arbeidsgivers IT-plattform skal være faglig begrunnet, og skal ikke utføres uten IKT personells godkjenning av installasjonen. Den ansatte er selv ansvarlig for konsekvensene ved egen installasjon.

Arbeidsgiver kan uten varsel fjerne programvare 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 arbeidsgivers utstyr (pc og lignende) og nettverk uten skriftlige godkjenning fra rådmannen eller den han godkjenner (IKT avdeling). F.eks. det er ikke tillatt å koble til mobiltelefon via kabel eller trådløs (bluetooth/infrarød) for å synkronisere data (f.eks. kalender). Det er ikke tillatt å sette opp eller inneha modemforbindelser eller ekstern tilgang uten spesiell godkjenning fra arbeidsgiver.

2.11. SPESIELT FOR SKOLENE

Lærer PC-er kan medbringes og disponeres hjemme hos den tilsatte lærer, herunder bruk av installert programvare og Internett/ e-post. Det er adgang til å koble pc-en opp mot egen skriver. I den grad programvare kan være til hjelp i undervisningen (f.eks. bildebehandling, lydredigering osv) tillates installasjon såfremt disse er nyttige og gratis tilgjengelig. Ved tvil skal dataansvarlig ved skolen eller IKT personell kontaktes og eventuelt godkjenne nedlasting/ installasjon.

2.12. INTERNETTBRUK

Internettbruk skal ta utgangspunkt i at all kommunikasjon på nettet kan spores tilbake til den maskinen du bruker (IP - adresse). Er du pålogget i arbeidstiden og benytter informasjonssystemet defineres du som pålogget i tjeneste.

All bruk på nettet blir loggført. Ved gjennomgang av logger som medfører innsyn i personopplysninger brukes samme metode for innsyn som ved e-post, se punkt 2.7.

Det anses som brudd på arbeidskontrakt å laste ned ulovlig materiale fra nettet uten at dette er godkjent av nærmeste leder som del av jobboppdrag. Under ingen omstendighet tillates nedlasting av ulovlig materiale som rammes av straffelovens §§ 204 og 204a (pornografi/barnepornografi). Det samme gjelder når det fra jobbmaskin gjøres forsøk på hacking eller annen uautorisert tilgang til andre informasjonssystemer.

Eksempel på akseptabel bruk:

Faglig oppdatering gjennom tilgjengelige nettmedia som lovdata, offentlige utredninger, bibliotekregister, nyheter og andre relevante kilder som for eksempel medisinske oppslagsverk/databaser. Å utveksle ikke sensitiv –faglig informasjon gjennom e-post.

Eksempel på uakseptabel bruk:

Å laste ned programvare og spill fra nettet med mindre dette er godkjent av IKT enheten. Installasjon av programvare med mindre det er godkjent av IKT enheten. Å laste ned pornografi, volds – og rasistisk preget materiale som kan virke usømmelig. Å utveksle personopplysninger og andre opplysninger av fortrolig karakter.

2.13. NÅR ANSATTE SLUTTER ELLER GÅR I PERMISJON

Minst 1 måned før en ansatt slutter eller går i lengre permisjon er det nærmeste **leders plikt å sørge for** at all informasjon/ alle dokumenter som vedkommende har lagret på sitt H-område eller i sin e-post blir vurdert av den ansatte. Arbeidsrelaterte dokumenter skal enten videreformidles leder eller arkiv. Vedkommende bruker skal meldes ut av datasystemet slik at brukertilgang og passord slettes ved fratredelsesdato. Det skal meldes fra om at vedkommende skal slettes som e-postadressat. Link til inn/utmeldingsskjema.

Er det berettiget mistanke om at ansatte ikke har etterkommet slik anmodning kan arbeidsgiver uten varsel gå inn på vedkommendes H-område og e-postsystem. Prosedyrene skal være som angitt foran i pkt. 2.6.

Ansatte som har bærbar PC, PDA , mobiltelefon eller minne - brikke skal levere dette tilbake **senest siste arbeidsdag**.

2.14. SANKSJONER

Konsekvenser ved Brudd på sikkerhetsbestemmelsene fremgår av punkt .1.4.

DEL 3 – INNHENTING AV PERSONOPPLYSNINGER

Del 3 i brukerinstruksen er spesielt myntet på medarbeidere som innhenter personopplysninger og sensitive personopplysninger fra innbyggerne eller ansatte i kommunen. Vedkommende skal kjenne til disse reglene og agere der etter.

3.1. INNHENTING OG KONTROLL AV DE REGISTRERTES SAMTYKKE (POL §§ 8, 9 OG 11)

3.1.1. VILKÅR FOR BEHANDLING AV PERSONOPPLYSNINGER

Personopplysninger kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller behandlingen er nødvendig for:

- å oppfylle en avtale med den registerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås
- at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse
- å ivareta den registrertes vitale interesser,
- å utføre en oppgave av allmenn interesse
- å utøve offentlig myndighet, eller at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til, kan ivareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.

3.1.2. BEHANDLING AV SENSITIVE PERSONOPPLYSNINGER

Sensitive personopplysninger kan bare behandles dersom behandlingen oppfyller et av vilkårene i pkt 3.1.1 og

a) den registrerte samtykker i behandlingen
b) det er fastsatt i lov at det er adgang til slik behandling
c) behandlingen er nødvendig for å beskytte en persons vitale interesser, og den registrerte ikke er i stand til å samtykke
d) det utelukkende behandles opplysninger som den registrerte selv frivillig har gjort alminnelig kjent
e) behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare et rettskrav

f) behandlingen er nødvendig for at den behandlingsansvarlige kan gjennomføre sine arbeidsrettslige plikter eller rettigheter
g) behandlingen er nødvendig for forebyggende sykdomsbehandling, medisinsk diagnose, sykepleie eller pasientbehandling eller for forvaltning av helsetjenester, og opplysningene behandles av helsepersonell med taushetsplikt
h) behandlingen er nødvendig for historiske, statistiske eller vitenskapelige formål, og samfunnets interesse i at behandlingen finner sted klart overstiger ulempene den kan medføre for den enkelte

3.1.3. GRUNNKRAV TIL BEHANDLING AV PERSONOPPLYSNINGER (POL § 11)

Som behandlingsansvarlig skal behandlingsansvarlig sørge for at personopplysningene som behandles:

a) bare behandles når dette er tillatt ref pkt 3.1.1. og 3.1.2
b) bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den resultatenhetens virksomhet
c) ikke brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker
d) er tilstrekkelige og relevante for formålet med behandlingen
e) er korrekte og oppdatert
f) ikke lagres lenger enn det som nødvendig ut fra formålet med behandlingen, jf. under pkt 4 om retting av mangelfulle personopplysninger og pkt 5 om forbud mot å lagre unødvendige personopplysninger.

Link til personvernombudets innmeldingsskjema for personopplysninger. Skjema sendes sikkerhetsansvarlig i kommunen som sender kopi av skjema til arkivtjenesten for oppbevaring og registrering.

3.2. VURDERING AV PERSONOPPLYSNINGENES KVALITET (POL §§ 11 BOKSTAV D OG E, 27 OG 28,)

Behandlingsansvarlig skal til enhver tid vurdere om personopplysningenes kvalitet er i samsvar med det definerte formålet med behandlingen av opplysningene i enhetens systemer.

Dette innebærer også at de ikke senere brukes til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker og at de er tilstrekkelige og relevante for formålet med behandlingen

Vurderingen gjelder også retting av mangelfulle personopplysninger og forbud mot lagring av unødvendige personopplysninger.

Oppfyllelse av begjæringer om innsyn og informasjon (pol §§ 16 til 24).

3.3. RETT TIL INNSYN (POL § 18)

3.3.1. GENERELT INNSYN

Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar, og kan kreve å få følgende informasjon om en bestemt type behandling:

a) navn og adresse på behandlingsansvarlig som behandlingsansvarlig og hans/hennes eventuelle representant
b) hvem som er saksbehandler
c) formålet med behandlingen
d) beskrivelser av hvilke typer personopplysninger som behandles
e) hvor opplysningene er hentet fra

f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.

3.3.2. SPESIELT INNSYN:

Dersom den som ber om innsyn er registrert, skal personvernombudet opplyse om:

- hvilke opplysninger om den registrerte som behandles
- sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten

Den registrerte kan kreve at personvernombudet utdyper informasjonen som er beskrevet over, i den grad dette er nødvendig for at den registrerte skal kunne ivareta egne interesser.

Personvernombudet kan kreve at den registrerte leverer skriftlig og undertegnet begjæring om innsyn. Den registrerte kan kreve å få informasjonen skriftlig.

3.3.3. SAKSBEHANDLINGSFRISTER

Saksbehandlingsfristen er 30 dager, men kan ved særlige forhold forlenges. Dette forutsetter et foreløpig svarbrev med varsel om behandlingstid og grunnen til forsinkelsen.

3.4. INFORMASJONSPLIKT (POL § 19)

Når det samles inn personopplysninger fra den registrerte selv, skal behandlingsansvarlig eller ansvarlig saksbehandler av eget tiltak først informere den registrerte om:

a) behandlingsansvarlig s navn og adresse og dennes eventuelle representant
b) formålet med behandlingen
c) opplysningene vil bli utlevert, og eventuelt hvem som er mottaker
d) det er frivillig å gi fra seg opplysningene
e) annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte, som f.eks. informasjon om retten til å kreve innsyn og retten til å kreve retting

Varsling er ikke påkrevd dersom det er på det rene at den registrerte allerede kjenner til informasjonen i første ledd.

3.5. UNNTAK FRA RETTEN TIL INFORMASJON (POL § 23)

Retten til innsyn og plikten til å gi informasjon omfatter ikke opplysninger:

a) om de ble kjent, ville kunne skade rikets sikkerhet, landets forsvar eller forholdet til fremmede makter eller internasjonale organisasjoner
b) det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger

c) det må anses utilrådelig at den registrerte får kjennskap til, av hensyn til vedkommendes helse eller forholdet til personer som står vedkommende nær. Disse opplysningene kan på anmodning likevel gjøres kjent for en representant for den registrerte når ikke særlige grunner taler mot det.
d) det i medhold av lov gjelder taushetsplikt for

e) utelukkende finnes i tekst som er utarbeidet for den interne saksforberedelse og som heller ikke er utlevert til andre
f) det vil være i strid med åpenbare og grunnleggende private eller offentlige interesser å informere om, herunder hensynet til den registrerte selv
g) Behandlingsansvarlig som nekter å gi innsyn i medhold av første ledd må begrunne dette skriftlig med presis henvisning til unntakshjemmelen.

4. MANGELFULLE OPPLYSNINGER – RETTING OG EVENTUELL SLETTING (POL § 27)

Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal behandlingsansvarlig av eget tiltak eller på begjæring av den registrerte sørge for at de mangelfulle opplysningene blir rettet. Behandlingsansvarlig skal om mulig sørge for at feilen ikke får betydning for den registrerte, f.eks. ved å varsle mottakere av utleverte opplysninger.

Retting av uriktige eller ufullstendige personopplysninger som kan ha betydning som dokumentasjon, skal skje ved at opplysningene tydelig markeres og suppleres med korrekte opplysninger. Det skal ikke brukes korrekturlakk el.

Dersom tungtveiende personvernhensyn tilsier det, kan Datatilsynet bestemme at retting skal skje ved at de mangelfulle personopplysningene slettes eller sperres. Hvis opplysningene ikke kan kasseres i medhold av arkivloven, skal Riksarkivaren høres før det treffes vedtak om sletting. Vedtaket går foran reglene i arkivloven 4. desember 1992 nr. 126 § 9 og § 18.

Sletting bør suppleres med registrering av korrekte og fullstendige opplysninger. Dersom dette ikke er mulig, og dokumentet som inneholdt de slettede opplysningene av den grunn gir et åpenbart misvisende bilde, skal hele dokumentet slettes.

5. FORBUD MOT Å LAGRE UNØDVENDIGE PERSONOPPLYSNINGER (POL § 28)

Behandlingsansvarlig skal sørge for at personopplysninger ikke lagres lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes.

Behandlingsansvarlig kan lagre personopplysninger for historiske, statistiske eller vitenskapelige formål, dersom samfunnets interesse i at opplysningene lagres klart overstiger de ulempene den kan medføre for den enkelte. Han/hun må da sørge for at opplysningene ikke oppbevares på måter som gjør det mulig å identifisere den registrerte lenger enn nødvendig.

Den registrerte kan kreve at opplysninger som er sterkt belastende for ham eller henne skal sperres eller slettes dersom dette:

a) ikke strider mot annen lov
b) er forsvarlig ut fra en samlet vurdering av bl.a. andres behov for dokumentasjon, hensynet til den registrerte, kulturhistoriske hensyn og de ressurser gjennomføringen av kravet forutsetter

Datatilsynet kan - etter at Riksarkivaren er hørt - treffe vedtak om at retten til sletting etter tredje ledd går foran reglene i arkivloven 4. desember 1992 nr. 126 § 9 og § 18.

Hvis dokumentet som inneholdt de slettede opplysningene gir et åpenbart misvisende bilde etter slettingen, skal hele dokumentet slettes.

6. OPPFYLLELSE AV PERSONOPPLYSNINGSLOVENS REGLER OM MELDE- OG KONSESJONSPLIKT, JF. PERSONOPPLYSNINGSLOVEN §§ 31 TIL 33.

Behandlingsansvarlig skal i forkant og innen 30 dager før behandlingen tar til, gi melding til personvernombudet via sikkerhetsansvarlig om:

- Behandling av personopplysninger med elektroniske hjelpemidler
- Opprettelse av manuelt personregister som inneholder sensitive opplysninger

Ny melding skal gis hvert 3. år. Krav til meldingens innhold er beskrevet i pol § 31.

Behandling av sensitive opplysninger som er avgitt uoppfordret, omfattes ikke av konsesjonsplikten. I tvilstilfeller kan behandlingsansvarlig kreve at datatilsynet avgjør om en behandling krever konsesjon.

7. FJERNSYNSOVERVÅKING (VIDEOOVERVÅKING)

Behandlingsansvarlig i en enhet som planlegger fjernsynsovervåking, må sørge for å avklare om denne er lovlig og eventuellt søke om konsesjon ihht. pol kap VII. Fjernsynsovervåking.

Ved fjernsynsovervåking skal behandlingsansvarlig sørge for at rutiner etableres og gjennomføres i samsvar med konsesjonen.

8. TILSYN OG KONTROLL

8.1. DATATILSYNET/PERSONVERNOMBUDET

Datatilsynet gir råd og veiledning og kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger blir fulgt, og at feil eller mangler blir rettet.

I Rana kommune er vi knyttet til personvernombudsordningen. Vårt personvernombud bistår med råd og veiledning og er den som skal motta alle innmeldingsskjema.

8.2. INTERNE OG EKSTERNE KVALITETSREVISJONER

Sikkerhetsrevisjonen skal:

- Undersøke i hvilken utstrekning virksomheten oppfyller de krav og retningslinjer som er nedfelt i kvalitetssystemet og som er pålagt virksomheten utenfra
- Undersøke behovet for forbedring og korrigering

9. VEDLEGG

VEDLEGG 1.
INFORMASJONSHÅNDTERING – RANA KOMMUNE.

Innledning

Dette dokument er et vedlegg til bruker instruks informasjonssikkerhet for ansatte i Rana kommune. Rutinen gjelder for informasjonshåndtering.

Klassifisering av informasjon

Informasjon som behandles i Rana kommune har forskjellig beskyttelsesbehov og er delvis regulert av lovverk. For at brukere skal kunne vite hvordan man skal håndtere informasjonen, gis det i dette

dokumentet definisjon av ulike typer informasjon, samt en tabell som viser hvordan den enkelte informasjon skal håndteres.

Følgende beskyttelsesgrader benyttes:

Klassifisering av informasjon	
Beskyttelses-grad	**Beskrivelse**
ÅPEN[1]	Åpen informasjon er informasjon som er åpent tilgjengelig for alle.
LAV (Rana kommune INTERNT)	Informasjon for internt bruk hvor kompromittering, tap eller utilgjengelighet kan føre til: ▪ Uønsket offentliggjøring i media av informasjon som bare skal være tilgjengelig for ansatte ▪ Mindre økonomiske tap. ▪ Mindre skade på Rana kommunes renommé. Eksempler på informasjon: Interne notater, rundskriv og presentasjoner
MIDDELS	Benyttes dersom det vil kunne *skade* offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende. Informasjon hvor kompromittering, tap eller utilgjengelighet kan føre til: ▪ At informasjon om Rana kommune som oppfattes som middels beskyttelsesverdig, kan bli lest/endret av uvedkommende. ▪ Skade på Rana kommunes renommé. ▪ Risiko for økonomiske tap - under kr. Eksempler på slik informasjon: Personopplysninger ,strategier, adgangskoder
HØY	Benyttes dersom det vil kunne forårsake *betydelig skade* for offentlige interesser, en bedrift, institusjon eller enkeltperson at informasjonen blir kjent for uvedkommende. Informasjon hvor kompromittering, tap eller utilgjengelighet kan føre til: ▪ At informasjon som oppfattes som sensitiv, kan bli lest/endret av uvedkommende. ▪ Alvorlig skade på Rana kommunes renommé. ▪ Risiko for økonomiske tap – over kr Eksempler på slik informasjon: ▪ Sensitive personopplysninger ▪ Sensitive opplysninger om virksomhetens strategi, planer og aktiviteter. ▪ Svært sensitiv informasjon om sikkerhetsrelaterte hendelser. ▪ Systempassord og andre passord
Unntatt .off	Unntatt offentlighet Brukes av offentlige etater. Man må henvise til hvilken paragraf dokumentet unntas etter.

[1] Dokumenter med åpen informasjon trenger ikke merkes med beskyttelsesgrad

Rutiner for informasjonshåndtering

	ÅPEN	LAV- (VIRKSOMH INTERNT)	Unntatt off.	MIDDELS	HØY
1. Merking					
Dokumenter / informasjon skal være merket med beskyttelsesgrad.		x	x	x	x
Dokumentet / informasjonen skal merkes med hvilken bestemmelse som gir hjemmel for å unnta dokumentet fra offentlighet.			x		
Angi eventuell tidsbegrensning for graderingen					
2. Kopiering					
Dokumenter skal bare kopieres til personer som har autorisasjon for graderingen.		x	x	x	x
3 . Oppbevaring					
Ethvert tap eller kompromittering av beskyttelsesverdige dokumenter skal meldes til Sikkerhetsansvarlig og nærmeste linjeleder.		x	x	x	x
Lagres på sikkert område på filsystem hvor kun den/de som skal ha informasjonen har tilgang			x	x	x
Forhindre innsyn fra utenforstående		x	x	x	x
Skal være nedlåst når ikke under oppsyn			x	x	x
Utskrifter					
Utskrifter skal hentes umiddelbart fra skrivere slik at konfidensialitet (”Need to know”) i saksbehandlingen opprettholdes			x	x	x
På reise/Hjemme:					
Dokumenter/elektroniske medier skal oppbevares under oppsyn av den ansatte eller avlåst			x	x	x
Lagres kryptert på bærbar PC, eller annet portabelt utstyr			x	x	x
4. Forsendelse/elektronisk håndtering					
Fysiske dokumenter (papir) sendes i posten i lukket konvolutt	x	x	x	x	x
Skal ikke overføres som e-post på Internett					x
Sendes som kryptert fil / kryptert vedlegg til e-post på Internett Sørg for å få kvittering fra mottaker om at e-posten er mottatt.			x	x	
Kan sendes som normal (ukryptert) e-post	x	x			
Tillatt å sende på telefax	x	x			
Informasjonen skal ikke kommuniseres på steder hvor samtale kan overhøres av utenforstående.			x	x	x
5. Journalføring					
Føres i journal unntatt offentlighet (ved mottak / forsendelse)			x	x	x

	ÅPEN	LAV- (VIRKSOMH INTERNT)	Unntatt off.	MIDDELS	HØY
Føres i åpen journal (ved mottak / forsendelse)	x	x	x[2]	x[2]	
6. Makulering av dokumenter					
Papir legges i egne makuleringsdunker		x	x	x	x
Papir kastes i papiravfall / avfall	x				
7. Håndtering av datalagringsmedia					
Disker, utstyr som inneholder harddisker og annet lagringsmateriale (f.eks. minnebrikker, backuptape etc.), skal leveres til IKT for forsvarlig destruksjon.	x	x	x	x	x
Lagringsmedia som CD, DVD og floppy-disker leveres til IKT for destruksjon			x	x	x
Lagringsmedia som CD, DVD og floppy-disker klippes/brekkes i biter ogkastes i avfall	x	x			
Reparasjon / Service*:*					
Datautstyr sendes IKT-kontoret	x	x	x	x	x

1 Hvis det føres offentlig journal, kan disse føres i åpen journal i stedet for journal unntatt offentlighet dersom journalføringen ikke røper fortrolige opplysninger. Nøytrale kjennetegn, utelatelser eller overstrykninger skal benyttes i kopi av journal som legges frem for publikum for å unngå at fortrolig informasjon røpes

Referanser

[1] Personopplysningsloven m. forskrifter
http://www.lovdata.no/all/nl-20000414-031.html

[2] Sikkerhetsinstruks –ansatte i Rana kommune

VEDLEGG 2.
RETNINGSLINJER FOR BEHANDLING AV E- POST RANA KOMMUNE.

1. Innledning.
Det er en overordnet målsetting at Rana kommune skal være en åpen, tilgjengelig og serviceorientert kommune. Elektronisk kommunikasjon skal benyttes både internt og eksternt for å ivareta dagens krav til hurtig kommunikasjon. Bruk av e-post er ett av flere virkemidler som bidrar til at dialogen med det offentlige kan skje på en helhetlig, enkel og brukerorientert måte.

Disse retningslinjene angir hvilke rutiner som gjelder for bruk av e-post som verktøy i Rana kommune. Formålet er å sikre at det etableres gode rutiner slik at lov- og regelverk etterleves, samtidig som man utnytter de muligheter for effektivitet og fleksibilitet som verktøyet gir.

2. Generelt
Microsoft Outlook brukes til å sende e-post både internt og eksternt over Internett til

adressater utenfor kommunens organisasjon. E- post til Rana kommune skal sendes til og håndteres av det ordinære postmottaket i kommunen. Følgende adressering brukes: postmottak@rana.kommune.no E-post kan også sendes direkte til enkeltpersoner. Hver bruker har definert adresse på formen:Fornavn.etternavn@rana.kommune.no . Det kan også etableres felles e-post adresser til enheter/virksomheter som betjenes av flere ansatte. Eksempel: servicetorget@rana.kommune.no.

All arkivverdig e-post som sendes til ansattes e-postadresse/ enhetsadresser skal oversendes arkiv for journalføring og arkivering fortløpende. Adressen til kommunens postmottak skal fremkomme på brev ark og hjemmeside. På nettsiden skal brukere oppfordres til å benytte kommunens offisielle e-postadresse for å sikre korrekt journalføring. Videre skal det fremgå at kommunen er forpliktet til å behandle alle dokumenter, inkludert e-post i samsvar med bestemmelsene i offentlighetsloven (lov av 19.juni 1970 nr. 69). Det betyr blant annet at alle saksdokumenter og korrespondanse til og fra kommunen som hovedregel er offentlig. Avsender må derfor være varsom med hvilken informasjon som sendes kommunen.

3. Avsender informasjon på kommunal e-post.
Rana kommunes standard e-post avsenderprofil skal benyttes av alle som har kommunal e-post adresse. Profilen lastes ned fra kommunens profilhåndbok som ligger på kommunens nettside: www.rana.kommune.no under meny punktet organisasjon. Innlogging: Brukernavn:demo. Passord: demo

4. Håndtering av inngående e-post.
E-post til sentralt postmottak skal åpnes av arkivtjenesten (arkivforskriften 3. 2.ledd)
Personlig adressert post videresendes direkte. Dersom en saksbehandler mottar arkivverdig e-post, skal denne videresendes til arkivtjenesten. Ved tvil kontakt Servicetjenesteavdelingen – arkiv. Den enkelte saksbehandler har **plikt** til å vurdere om posten må anses som et arkivverdig dokument.

Arkivverdig e-post som kommer til postmottak skal journalføres av arkivtjenesten før den omdeles. Arkivtjenesten må ta stilling til om meldingen, vedlegget eller begge deler skal journalføres og tilknyttes dokumentregistrering i journalsystemet (se egne rutiner).

Ikke arkivverdig e-post vurderes/arkivbegrenses:

- ikke arkivverdig – slettes / eller arkiveres på egne / eventuelt private mapper.
- øvrig videresendes uten journalføring
- av interesse for saksbehandler – kan oppbevares

5. Videresending av inngående e-post
Når inngående e-post skal videresendes til flere ansatte, skal en person innsettes som hovedmottaker, de andre settes inn som kopimottakere. Hovedmottaker er ansvarlig for e-posten.

6. Verifisering av mottatt e-postforsendelser.
Hvis det er tvil om e-postmelding kommer fra den oppgitte avsender eller at avsender ikke er entydig identifiserbar, skal det umiddelbart sendes en tilbakemelding pr. e-post til oppgitt avsender, hvor det bes om verifisering av avsender. Arkivtjenesten må undersøke om vedlegg til e-postforsendelsen er i riktig format og lesbar. Dersom vedlegget ikke er lesbart, må avsender varsles med informasjon om hvilke formater som kan leses. Vedlegg virussjekkes (automatisk)

7. **Kvittering for mottak av e-post.**
Det skal ikke benyttes automatisk kvittering for mottak av e-post. Det er saksbehandlers ansvar å gi tilbakemelding innen 3 dager til mottaker om at e-posten er mottatt. (ikke det samme som frist etter Fvl – 21 dager)

8. Håndtering av utgående e-post.

Arkivverdig utgående e-post skal journalføres og arkiveres i kommunens elektroniske arkivsystem før det ekspederes.

9. Taushetsbelagte opplysninger.
Opplysninger som er underlagt lovbestemt taushetsplikt i henhold til offentlighets loven skal ikke sendes som e-post. Unntak kan gjøres dersom personopplysninger anonymiseres, slik at det ikke er mulig å knytte opplysningene til enkeltpersoner eller hvis forsendelsen er kryptert.

10. E-postrutiner ved saksbehandlers fravær.
Saksbehandler må sikre at mottatt e-post kan behandles også ved fravær over lengre tid. Dette skal gjøres ved bruk av fraværsassistenten i e-postsystemet for automatisk svar med opplysninger om fraværets varighet. Adresse for kommunens postmottak skal oppgis.

Eksempel på automatisk svar:
Jeg er ikke tilstede på kontoret før tirsdag 18. april.
Din e-post til meg - vil først bli lest da.
Meldinger som må behandles før jeg er tilbake - må sendes på nytt til
postmottak@rana.kommune.no

Når du selv får en slik melding om fravær, er det viktig å åpne denne e-posten. Spesielle opplysninger som saksbehandler har skrevet leses i åpnet e-post.
På mail adresser til enheter der flere ansatte er tilknyttet må det etableres rutiner slik at inngående e-post effektueres fortløpende.

11. **Arbeidsgiversadgang til ansattes e-post og oversikt over bruk av e-postsystemet.**
Lov om personopplysninger, forskrifter til denne loven, samt Datatilsynets retningslinjer regulerer adgang til ansattes e-post og andre elektroniske dokumenter.

<u>Utdypende kjøreregler</u>

1. Informasjon og henvendelser skal i hovedsak følge linja. Henvendelse til rådmann skal skje fra produksjonsleder. Henvendelse til ordfører skal skje via rådmann.
2. Det skal ikke sendes sensitive personopplysninger med elektronisk post. Slik e-post skal ikke distribueres videre, kommenteres eller besvares.
3. Ved planlagt fravær ut over tre dager skal fraværsassistenten benyttes. Se pkt.10. - retningslinjer for håndtering av e-post.
4. Det er den enkeltes ansvar og plikt å gå igjennom sin elektroniske postkasse. Innfør den vane å åpne postkassen din når du kommer på jobb.
5. Som en ekstra sikkerhet mot innsyn i private opplysninger, oppfordres ansatte til å merke e-post med privat innhold med ”privat”, eventuelt opprette en mappe merket ”privat” for denne type e-post.

6. Ved lengre fravær kan Rana kommune åpne saksbehandlers e-post og internt informasjon for å få tilgang til viktig informasjon. Rana kommune skal kontakte saksbehandler før dette skjer.
7. Dersom det er umulig å varsle saksbehandler, skal det alltid være to personer tilstede ved åpning av e-post. Nærmeste leder er ansvarlig for å dokumentere hva som er gjort.
8. Ved åpning av ansattes e-post konto skal dette skje av postmottak/ nærmeste leder/ arkivfunksjon/ IT-ansvarlig og eventuelt tillitsvalgt.
9. E-post i mappe merket privat eller e-post som tydelig er av privat karakter skal ikke åpnes av andre enn saksbehandler.
10. Rana kommune skal gi ansatte opplæring slik at de er i stand til å følge disse reglene.
11. Ikke videresend kjedebrev eller virusadvarsler
12. Ikke send e-post til veldig mange personer samtidig

13. Ikke send vedlegg du ikke vet om mottakeren kan lese
14. Ikke send store filer som vedlegg (vis heller til nedlastingsside på nettet)
15. Send e-post som ren tekst, ikke som HTML eller tilsvarende
16. Internt brukes intranettet *"på innsia"* som hovedinformasjonskanal.

Gode råd for e-post:

- Skriftlig kommunikasjon er vanskelig
- Sitér riktig når du svarer på e-post
- E-post er like alvorlig som annen post
- E-post er ikke noe mindre alvorlig enn annen post, så ikke tro at du kan sende hva som helst og unnskylde deg med, "Det er jo bare en e-post".
- Bruk e-post med tilstrekkelig aktsomhet. E-post må, forutsatt at den ikke er kryptert, betraktes å være relativt lett tilgjengelig for uvedkommende.
- Ha en profesjonell tone og vær objektiv – unngå sterke følelsesmessige uttrykk.
- Vær nøyaktig og faktaorientert – presiser eventuell usikkerhet.
- Sørg for fullstendighet – fremstill hele bildet.
- Ikke ta parti mot den du representerer, verken i sak eller i enkeltspørsmål.
- Ikke skriv nedsettende om andre, unngå sleivete humor.
- Hvordan vil en uavhengig tredjepart senere tolke det du skriver.
- Begrens antall mottakere. Tenk etter om meldingen er relevant for alle mottakerne.
- Begrens innholdet. La en melding bare omfatte et emne hvis mulig. Det er bedre med flere korte meldinger enn en lang.
- Mange sender Excel- og Word-dokumenter som vedlegg, uten å tenke på at mange mennesker ikke har mulighet til å åpne dem. Send derfor ren tekst, eller PDF dersom du har bilder og grafiske elementer i dokumentet ditt.
- Vær flink til å rydde i e-postkassen din. Husk at det er mange andre som bruker den samme e-postserveren, og det er ikke ubegrenset med plass der.
- Fare for virus. Vær kritisk til vedlegg du mottar, særlig fra ukjente personer eller hvis du ikke spesielt har bedt om å få filen det er snakk om. Svært utbredte e-postklienter som Outlook og Outlook Express har større sjanse for å bli angrepet av virus enn andre, mindre brukte e-postklienter.
- Ikke skriv når du er sint eller opprørt. Husk: Du kommuniserer med andre mennesker.
- Alt du skriver kan brukes mot deg.

10. EGENERKLÆRING

Jeg bekrefter herved å ha lest og forstått brukerinstruks IKT for Rana kommune

---------- ----------

Navn og fødselsdato (6 siffer) Dato