

# IT-reglement:

## **Del 1:**

Overordnet reglement for bruk av IT

## **Del 2:**

- Reglement for utnyttelse av IT-ressurser
- Reglement for brukerregistrering
- Reglement om plikt til å identifisere seg
- Reglement om eierskap og utlevering av data
- Reglement for utlevering av logger eller liknende informasjon
- Reglement for iverksetting av sanksjoner mot brukere
- Reglement for inngrep fra driftspersonalets side
- Reglement om saksbehandling

# Overordnet reglement for bruk av IT

## Nedslagsfelt:

Dette reglementet gjelder for bruk av universitetets IT-ressurser. Reglementet gjelder også bruk av andres IT-ressurser gjennom bruk av sin tilknytning til universitetet.

## Bruk av IT-ressurser:

Bruk av universitetets IT-ressurser er ment å skulle oppfylle universitetets formål. Det er forbudt å bruke universitetets IT-ressurser til noe som er uforenlig med universitetets formål, eller med de etiske eller moralske normene som er fastsatt for universitetet. Bruk av universitetets IT-ressurser til noe som strider mot norsk lov vil kunne føre til selvstendige sanksjoner fra universitetet.

Det er ikke tillatt å bruke universitetets IT-ressurser uten å få tillatelse til dette i forkant. Det å få en bruker hos institusjonen innebærer at tillatelse er gitt til formålstjenlig bruk.

Det er ikke tillatt å bruke universitetets IT-ressurser på en måte som opptar større ressurser enn nødvendig, tatt de tilgjengelige ressursene i betraktning. Bruk som ikke er begrunnet i universitetets formål skal ikke oppta annet enn ubetydelige ressurser.

IT-ressursene skal ikke brukes på en måte som kan forringe eller krenke deres integritet. Dette gjelder også ved bruk av privat utstyr.

Brukere har plikt til å følge IT-ansattes pålegg og instruksjoner om bruk av IT-ressursene. Hvor det er påkrevd skal brukere identifisere seg på korrekt måte. En brukers passord eller annen nøkkel skal holdes hemmelig og skal kun anvendes av den korrekte brukeren.

Vis nett-vett.

## Brukernes rettigheter

Universitetet skal sette klare standarder og retningslinjer for hva som er forsvarlig bruk av universitetets IT-ressurser.

Universitetet skal tilgjengeliggjøre oppdatert informasjon til brukerne om relevante forhold om IT-ressursene og brukernes anvendelse av disse.

Alle brukere har krav på at deres personvern og integriteten til deres data ikke krenkes av universitetet. Universitetet skal bidra til for at brukernes personvern og integriteten til brukernes data ikke krenkes av andre.

Universitetet skal ikke utlevere opplysninger om en enkelt bruker eller data tilhørende en bruker hvor dette ikke fremgår av vedtatte reglementer eller følger av lovgivningen forøvrig.

## Inngrep og sanksjoner

Brudd på IT-reglementet kan føre til sanksjoner fra universitetet. Straff eller sanksjoner grunnet bruk av IT-ressurser skal ikke avvike fra sanksjoner grunnet annen opptreden ved universitetet. Sanksjoner skal fastsettes av ansvarlig enhet.

IT-driftspersonell har som oppgave å sikresystemets funksjonalitet og integritet. IT-driftspersonell ved universitetet kan utføre ethvert inngrep for å ivareta systemets funksjonalitet så lenge som det ikke er i utrensmål Ved inngrep skal bruker varsles så snart som praktisk mulig.

## Ansvarsfraskrivelse:

Universitetet er ikke ansvarlig for noe tap av data, tjenestebortfall eller andre tap som skyldes svikt i IT-tjenestene. universitetet kan ikke frata brukere rettigheter eller stille dem til ansvar grunnet handlinger eller passivitet hvor det er svikt i IT-tjenestene som er årsaken til dette.

<b>Reglement</b>	<b>Dato</b>	<b>Gitt av</b>	<b>Hjemmel</b>
Utnyttelse av IT-ressurser		Styret	

## **Utgangspunkt.**

Bruk av universitetets IT-ressurser skal hovedsakelig forekomme for å fremme universitetet formål. Det er ikke tillatt å bruke universitetets IT-ressurser på en måte som opptar større ressurser enn nødvendig, tatt de tilgjengelige ressursene i betraktning. Bruk som ikke er begrunnet i universitetets formål skal ikke oppta annet enn ubetydelige ressurser.

## **Tillatt bruk etter universitetet formål.**

Formålet til universitetet er utdanning, forskning og formidling.

Bruk som er direkte relatert til universitetet formål er grunnlaget for de ressursene som er tilgjengelige og er derfor tillatt så lenge som det ikke opptar for store ressurser slik at bruken blir til fortrensel for annen tillatt bruk.

Bruk som ikke er direkte relatert til universitetet formål er kun tillatt i den utstrekning det opptar ubetydelige ressurser. Bruk som ikke har noen beskyttelsesverdige interesse kan forbys av IT-avdelingen.

## **Privat bruk**

IT-tjenestene ved universitetet er hovedsakelig til bruk for å oppfylle formålet til universitetet. Imidlertid er det fullt ut akseptabelt at brukere anvender IT-ressursene til private gjøremål så lenge som de ikke

- opptar IT-ressurser på bekostning av annet bruk.
- bryter lisenser, avtalevilkår eller andre forutsetninger
- bidrar til å svekke sikkerhet eller stabilitet
- er forbudt av IT-avdelingen

## **Kommersiell bruk**

Bruk av universitetet IT-ressurser til kommersielle formål (enhver form for kjøp, salg, utleie, annonsering mot betaling eller likende) er forbudt med mindre det foreligger skriftlig tillatelse til slik bruk i forkant.

## **Bruk med ingen beskyttelsesverdige interesse**

Handlinger som anvender IT-ressurser men ikke er begrunnet utifra beskyttelsesverdige interesser slik som universitetets formål eller alment aksepterte interesser kan forbys av IT-avdelingen. Hvor det er grunn til å klandre brukeren for handlingen kan sanksjoner iverksettes. Avveigingen skal foretas etter momentene gjengitt under:

En handling har ikke beskyttelsesverdige interesser i denne konteksten hvor den ikke har en særlig nærhet til universitetets formål og heller ikke har en særlig nærhet til alminnelig anerkjente

rettigheter eller formål slik som:

- demokrati
- grunnleggende rettigheter
- samfunnsøkonomisk nytte
- tekniske eller andre vitenskapelige fremskritt

Handlingen vi kunne være i strid med dette reglementet hvor den samtidig anvender universitetets IT-ressurser.

IT-avdelingen kan iverksette sanksjoner mot en bruker som har foretatt en slik handling hvor:

- En vanlig oppegående bruker forsto eller burde ha forstått at handlingen ikke var tillatt bruk av IT-ressursene

og

- Handlingen ikke utelukkende eksisterte i brukersens privatsfære.

## **Håndheving av ressursutnyttelse.**

Enhver enhet og hver enkelt bruker har et selvstendig ansvar for å selv påse at eget bruk er innenfor grensene av tillatt bruk. IT-avdelingen kan og skal gi generelle retningslinjer om hvilket bruk som tillates.

I spesielle tilfeller hvor IT-avdelingen blir oppmerksom på bruk som, etter en konkret vurdering basert på nærheten til universitetets formål, andre beskyttelsesverdige interesser og mengden ressurser bruken opptar, ikke bør tillates, skal IT-avdelingen sørge for at denne stoppes. Hvis det er grunn til å klandre en bruker for opptreden i forbindelse med slik bruk kan sanksjoner fra IT-avdelingen iverksettes mot brukeren.

<b>Reglement</b>	<b>Dato</b>	<b>Gitt av</b>	<b>Hjemmel</b>
<b>Reglement for Brukerregistrering</b>		Styret	

### **Vilkår for å bli bruker**

For å bli bruker ved universitetet må man ha et formalisert forhold til institusjonen. Et formalisert forhold har den som er ansatt, opptatt til studier eller har en skriftlig avtale med institusjonen om sin tilstedeværelse.

For å bli bruker skal et minimumssett av ens persondata finnes i et av de administrative systemene til Institusjonen. Dette kan være studentsystemet eller personalsystemet. De opplysningene som må registreres er:

- navn
- personnummer
- tilknytning / rolle i forhold til institusjonen
- varlighet på tilknytning
- plassering i institusjonen

Visse typer ansatte kan ha en tilknytning som ikke etter sitt formål behøver å bli bruker av IT-tjenestene. Dette skal i så fall være grunnet objektive kriterier og utvelgelse skal skje på grunnlag av formelle roller. Dette skal fremgå av registreringen i student eller personalsystemet.

### **Registrering av brukere**

Ved registrering av nye individer i enten student eller personalsystem skal det automatisk bygges en bruker til vedkommende. Dette gjelder ikke hvis:

- *det av vedkommendes registrering fremgår at denne ikke skal ha bruker*
- *det allerede finnes en bruker for et individ med den identifikatoren*

Finnes det allerede en bruker og denne skal benyttes, må det sikres at de over nevnte pliktige personopplysninger er tilstede i oppdatert form.

Etter at bruker er bygget skal brukernavn og passord (eller annen autentiseringsinformasjon, f.eks. pin-kode) sendes bruker på sitt arbeids/studiested. Samtidig skal bruker få informasjon om IT-ressursene og reglene for bruk av disse.

IT-avdelingen skal som regel ikke bygge brukere som ikke finnes i enten student eller personalsystem. Unntak fra dette kan skje hvor tekniske forhold nødvendiggjør det. Ved manuell registrering skal også de over nevnte pliktige personopplysninger registreres. Manuelt opprettede brukere skal ikke være gyldige i mer enn ett år.

Det kan settes som vilkår at bruker ved første anvendelse / aktivering av brukerkonti selv velger et nytt passord/pinkode el. l.

## **Varighet av brukerforhold**

En brukers konto ved universitetet skal ha en like lang varighet som tilknytningen brukeren har til institusjonen har. I tillegg kan brukeren få tre måneder til å rydde opp i sine forhold før kontoen blir sperret.

## **Opphør av brukerforhold**

Ved opphør av brukerens tilknytning etter registrering enten student eller personalsystem skal brukeren varsles om at kontoen sperres om 3 måneder og at brukeren i denne perioden må ta sikkerhetskopi av alle filer brukeren ønsker å beholde<sup>1</sup>.

Etter 3 måneder sperres brukerens konto. Etter ytterligere seks måneder slettes brukerens konto. Sikkerhetskopierte data slettes etter 5 år.

---

<sup>1</sup> Se «eierskap til data»

<b>Reglement</b>	<b>Dato</b>	<b>Gitt av</b>	<b>Hjemmel</b>
<b>Brukerens plikt til å identifisere seg</b>		Styret	

## **Korrekt identifikasjon**

Alle brukere plikter å til enhver tid identifisere seg selv på en korrekt måte ovenfor institusjonen hvor det er lagt opp til dette. Det er forbudt å identifisere seg eller å forsøke å identifisere seg som en annen enn den man er.

### **Riktig brukernavn**

For alle tjenester hos universitetet hvor en skal identifisere seg selv skal kun ens eget brukernavn anvendes.

### **Riktig avsenderadresse**

Det er forbudt å forsøke å modifisere eller skjule noen felt eller informasjon i noen kommunikasjon med sikte å å skjule hvor den kommer fra, eller gi et feilaktig bilde av dette.

### **Riktig maskinnavn/ip adresse**

Det er forbudt å forsøke å endre en innstilling, aksessere tjenester via omveier eller på andre måter forsøke å skjule hvilken maskin en sitter ved eller gi et feilaktig inntrykk av dette ovenfor universitetet eller andre brukere tilknyttet universitetet.

## **Hemmeligholdelse av nøkkel**

Det er svært viktig å holde sin nøkkel hemmelig. Denne eksistere ofte i form av et passord eller en pin-kode. Det er forbudt å dele denne med noen. Hvor det går frem at en nøkkel er blitt kjent vil brukerkonto bli sperret og brukeren vil bli ansvarliggjort.

## **Rett til anonymitet**

Det er ikke opp til institusjonen å bestemme hvorvidt brukerne identifiserer seg ovenfor 3. mann ved bruk av åpnet tjenester utenfor universitetet. Dog vil brudd på norsk eller internasjonal lovgivning utført via eller ved hjelp av universitetet IT-ressurser rammes at IT-reglementet.

<b>Reglement</b>	<b>Dato</b>	<b>Gitt av</b>	<b>Hjemmel</b>
<b>Eierskap og utlevering av data</b>		Styret	

***Dette reglementet dekker ikke logger ol. som er institusjonens eiendom.***

## **Utgangspunkt:**

Universitetet forholder seg til en fil eier som en indikasjon på hvem som eier data. Om eierskapet er korrekt eller ikke skal ikke dette på noe vis endre det reelle eierskapet til data.

## **Eierskap til data**

Universitetet forholder seg til at den som er oppført som eier av en fil er denne datas eier. Dette uansett hvor filen skulle befinne seg. Universitetet vil kun utlevere filen til den som er oppført som eier med mindre det ved beslutning av norsk domstol bestemmes noe annet.

### **Konflikt om eierskap til data mellom to 3. parter**

Hvor to parter begge hevder å være eier til data vil universitetet i utgangspunktet utlevere data til parten som er oppført som eier av filen. Hvor en part varsler rettslige skritt for å få fastslått eierskapet kan universitetet allikevel i en kortere periode avvente utleveringen.

### **Hvis ikke en avgjørelse fattes, får ingen utlevert noe?**

Hvor det ikke er mulig å sannsynliggjøre hvem som eier data, og flere hevder å ha eiendomsretten til nevnte data, vil det ikke bli utlevert noe før det foreligger en avgjørelse fra norsk domstol omkring eierskapet til dataene.

## **Utlevering av data ved brukerforholdets opphør**

### **Brukerforholdets opphør grunnet brukerens tilknytning til universitetet**

Hvor brukerens forhold til universitetet opphører, f.eks. ved endt studium eller avsluttet arbeidsforhold skal brukeren selv besørge å fjerne sine data fra universitetet IT-ressurser, herunder å ta kopier av de data brukeren ønsker å beholde. Brukeren skal derfor ha tilgang til sine data i tre måneder etter at rollen som begrunnet brukerforholdet opphørte. I løpet av denne perioden må brukeren motta varsel om at kontoen vil bli slettet og at alle data vil forsvinne. Etter dette skal universitetet vente i ytterligere tre måneder før kontoen inklusive all data blir slettet.

At brukeren skal ha tilgang til sine data betyr ikke at andre tjenester skal være tilgjengelige.

## **Brukerforholdets opphør grunnet brukers død**

Hvor en bruker dør, vil dennes arvinger (dødsboet) tre inn i dennes sted hva angår rettigheter knyttet til såvel fysiske som immaterielle goder og objekter. Retten til innholdet av dennes hjemmeområde er et slikt.

Det som må fastlegges er at den eller de som ønsker å få utlevert innholdet av hjemmeområdet er rett arving. Dette gjøres ved fremleggelse av en skifteattest, hvor det fremgår hvem arvingene er.

Personlig innhold skal lagres på hjemmeområde. Materiale som lagres på arbeidsplassmaskin vil uten gjennomgåelse av hva det inneholder bli slettet ved en brukers død.

## **Prosedyre for utlevering av data**

### **Utfylling av erklæring**

Utlevering skjer mot utfylling av en erklæring hvor mottaker av data underskriver på at denne

- Har mottatt data
- Erkjenner at overleveringen ikke medfører noen endring i faktiske eierforhold.
- Lover å utlevere data som tilhører andre til riktig mottaker

### **Arkivering**

En kort redegjørelse (f.eks en logg) for utleveringen, samt kopi av dokumenter som identifiserer rett mottaker (f.eks. skifteattest), erklæring og andre relevante dokumenter skal arkiveres.

### **Utlevering**

Utlevering skjer på egnet medium som kan deles ut i bytte mot erklæring.

<b>Reglement</b>	<b>Dato</b>	<b>Gitt av</b>	<b>Hjemmel</b>
<b>Utlevering av logger eller liknede informasjon</b>		Styret	

## **Utlevering av opplysninger**

Det vil med jevne mellomrom kunne komme klager eller henvendelser rettet til institusjonen hvis mål er å få utlevert logger eller informasjon (identitet) om en bruker. Dette er i utgangspunktet ikke noe man skal gi ut. Mange av opplysningene er belagt med taushetsplikt, men også andre regler, f.eks. etter personopplysningsloven tilsier at stor forsiktighet skal utvises i forhold til utlevering av informasjon om enkeltpersoner eller om deres bruk av IT-ressurser.

## **Spesielt om utlevering til politi eller påtalemyndighet**

Etter Ekomlovens §2-9 kan politi eller påtalemyndighet kreve å få identifisert en bruker av et ip-nummer. Andre data, f.eks. logger av trafikkdata eller innholdet i kommunikasjoner krever beslutning av en domstol.

## **Utlevering til andre**

Utlevering opplysninger, logger eller likende til andre enn politi eller påtalemyndigheter krever beslutning fra norsk domstol.

## **Utlevering til brukeren selv**

En bruker som ønsker utlevert seg opplysninger, logger eller likende som omhandler denne selv kan få dette ved vanlig henvendelse til IT-avdelingen. Retten til dette følger bla. av personopplysningsloven.

## **Fellestjenester i sektoren**

For fellestjenester i sektoren, herunder en brukers utnyttelse av andre institusjoners IT-ressurser vil eventuelt misbruk enten bli tatt hånd om av brukerens vertsinstitusjon ved klage på denne fra institusjonen hvis ressurser er misbrukt, eller institusjonen hvis ressurser er misbrukt kan forfølge saken i rettsvesenet og dermed få identifisert brukeren etter reglene over.

<b>Reglement</b>	<b>Dato</b>	<b>Gitt av</b>	<b>Hjemmel</b>
<b>Sanksjoner mot brukere</b>		Styret	

## **Sanksjoner**

En sanksjoner en reaksjon iverksatt for å straffe en bruker for klanderverdig adferd fra dennes side. Handlingen iverksatt for å oppnå andre resultater, f.eks. stabilitet og sikkerhet blant IT-ressursene er ikke en sanksjon.

Sanksjoner i forhold til opptreden relatert til IT-ressurser skal håndteres av IT-organisasjonen. Sanksjoner relatert til annen opptreden skal håndteres av brukerens ansvarlige enhet.

## **Omfang av sanksjoner og kompetanse til å iverksette disse**

### **Styret**

En total sperring av en brukerkonto er en bortvisning etter universitetslovens §11.

Styret er tillagt kompetansen til å bortvise en bruker. Saksbehandlingen og prosedyren for å gjøre dette er bestemt av lovverket. Disse må følges i slike tilfeller.

Retten til å ha en operativ brukerkonto som gir tilgang til administrative tjenester, undervisning og tilhørende innleveringer eksamener mv. kan ikke som en sanksjon fratras brukere uten at dette er å anse som en bortvisning. Det samme gjelder retten til å kunne motta kommunikasjon fra universitetet eller noen av dens organer.

### **Ansvarlig enhet**

Den ansvarlige enheten skal ikke iverksette sanksjoner ved hjelp av. endring av privilegier for bruk av IT.

### **IT-organisasjonen**

IT-avdelingen kan iverksette sanksjoner ved å frata brukere visse begrensede privilegier i en begrenset tidsperiode.

Sanksjoner skal være et resultat av et misbruk og relatert til den misbrukte ressursen.

Førstelinde av IT-organisasjonen skal ikke iverksette sanksjoner mot brukere utover tilsnakk eller rapportering av dem til 2. linje.

Ved alvorlig misbruk skal IT-avdelingen eskalere en sak i linjen, via den ansvarlige enheten til Styret, for beslutning om bortvisning skal finne sted.

<b>Reglement</b>	<b>Dato</b>	<b>Gitt av</b>	<b>Hjemmel</b>
<b>Inngrep</b>		<b>Styret</b>	

## **Inngrep**

Et inngrep er en faktisk handling som er foretatt for å oppnå noe annet enn å straffe en bruker.

IT-avdelingen kan foreta inngrep når dette er nødvendig. Med nødvendig menes for å opprettholde integritet, konfidensialitet og tilgjengeligheten i IT-systemer, tap av liv helse eller gods, hindre at universitetet kommer i ansvar, eller opprettholdelse av universitetet rykte samt det å forhindre rettsbrudd.

## **Innsyn**

Med innsyn menes en fysisk individ som gjennom en manuell prosess skaffer seg tilgang til data som tilhører andre brukere. Automatiske prosesser som foretar handlinger mot store grupper brukere bedriver ikke innsyn. Dette gjelder f.eks. virusscanning eller prosesser som generer rapporter som ikke identifiserer individer.

### **Filer, områder og logger**

Brukrens private sfære strekker seg til kunnskap om eksistens av og innhold i filer. Hvilke prosesser en maskin har gående er informasjon som til enhver til skal være tilgjengelig for driftspersonale.

Logger som inneholder informasjon om prosesser, innlogginger, avvik eller andre hendelser er institusjonens eiendom og skal være tilgjengelig for driftspersonale.

Det er et konkret skille mellom brukerens filer og områder, og den logging av diverse ting som en institusjon foretar. Det er ikke et innsyn i så måte å gå gjennom disse, men det må til gjengjeld være slik at institusjonen ikke logger annet enn det som er forsvarlig, og at dette opplyses om.

## **Innsyn i data, filer eller områder tilhørende privat bruker**

Det er i utgangspunktet kun brukeren selv som har tilgang til dennes data, filer eller private områder.

### **Samtykke**

Som standard er samtykke det man skal be om hvis inngrep med innsyn er nødvendig.

I visse tilfeller kan det være nødvendig å skaffe seg dette uten samtykke.

### **Tillatelse fra overordnet**

I en situasjon hvor tidsnød eller andre årsaker umuliggjør eller gjør det svært vanskelig eller uhensiktsmessig å innhente samtykke kan innsyn foretas med tillatelse av IT-Direktøren eller den som opptre i dennes sted.

## **Situasjoner med særlig tidsnød**

I en situasjon hvor særlig tidsnød eller andre årsaker umuliggjør eller gjør det svært vanskelig eller uhensiktsmessig å innhente tillatelse av IT-Direktøren eller den som opptrer i dennes sted, kan innsyn foretas av IT-personale

## **Informasjon i ettertid**

Hvor noen har skaffet seg innsyn i en brukers personlige område uten forutgående samtykke fra brukeren selv skal brukeren straks varsles.

Varslet skal redegjøre for hvilket inngrep som har blitt foretatt, hvilken hjemmel dette hviler på og de særlige forhold som er påberopt.

## **Registrering av innsyn**

At innsyn har vært foretatt skal registreres i saksbehandlingssystem.

## **Sperring/stengning av ressurser**

Hvor et det er nødvendig kan inngrep iverksettes ved å sperre, stenge eller på andre måter endre en ressurs.

## **Informasjon til brukere**

Hvor en ressurs sperres skal brukeren ha beskjed. Dette skal skje så snart som mulig. Hvor ressurser som påvirker mange brukere er sperret kan innholdet i varsel være identisk. Hvis det er praktisk mulig bør informasjonen nå alle brukere individuelt. Beskjed skal gis gjennom et kommunikasjonsmiddel som ikke er sperret.

<b>Reglement</b>	<b>Dato</b>	<b>Gitt av</b>	<b>Hjemmel</b>
<b>Saksbehandling</b>		Styret	

## **Alminnelige regler ved saksbehandling**

IT-ansatte er underlagt de alminnelige saksbehandlingsreglene som gjelder i det offentlige hva angår utøvelse av myndighet som ansatt av forvaltningsorgan.

### **Taushetsplikt**

IT-ansatte er underlagt taushetsplikt etter forvaltningslovens § 13. Taushetsplikten gjelder for alle taushetsbelagte opplysninger som en får kjennskap til gjennom utøvelse av sin stilling. Taushetsplikten gjelder også mot andre ansatte i IT-organisasjonen, unntatt oppover i linjen.

### **Arkiveringsplikt**

Dokumenter tilhørende sak hvis behandling utgjør et enkeltvedtak etter forvaltningsloven § 2 litra b er arkivverdig og skal arkiveres i offentlig journal. Ved tvil om hvorvidt en sak er arkivverdig eller ei skal arkivpersonale rådføres.

### **Innsynsrett**

Alle har rett til innsyn i offentlig journal jmf. offentlighetsloven § 2.

Alle som er part i en sak har innsyn i sakens dokumenter. Innsynet gjelder ikke dokumenter og kommunikasjon for intern saksforberedelse.

### **Svarplikt mm.**

universitetet plikter å besvare alle henvendelser rettet til det som forvaltningsorgan eller institusjon. Dette gjelder ikke masseutsendte kommunikasjoner i markedsføringsøyemed (SPAM).

Alle henvendelser skal besvares innen rimelig tid.

universitetet plikter å gi alminnelig veiledning til brukerne som er relevant i forhold til mottatte henvendelser. Slik veiledning kan være henvisning til tilgjengelig informasjon. I saker hvor det utøves forvaltningsmyndighet skal det fremgå at brukerne har adgang til å klage på enkeltvedtak.

Gjentatte henvendelser i saker hvor som er avgjort og hvor det ikke er videre klageadgang er ikke tillatt. Ei heller gjentatte meningsytringer til slike kanaler, hvor svar på slike allerede har blitt gitt. Det er ikke pliktig å besvare slike henvendelser annet enn med enstandardisert avvisning.

### **Elektronisk kommunikasjon**

Det skal fremgå tydelig, for eksempel på institusjonens hjemmeside, hvilke kanaler og adresser som kan benyttes til å rette henvendelser til institusjonen ved hjelp av elektronisk kommunikasjon. Institusjonens angitte inngående kommunikasjonskanaler skal leses av ikke være gjenstand for maskinell fjerning av kommunikasjoner.