

IT-regler gældende for Danmarks Journalisthøjskole

Retningslinjer for studerende og medarbejdere ved Danmarks Journalisthøjskole vedrørende brugen af højskolens IT-ressourcer

Indhold

1. Formål med IT-reglerne	2
2. Hvem er omfattet af IT-reglerne	2
3. Hvad er omfattet af IT-reglerne	2
4. Generelle regler vedr. brugen af DJHs IT-ressourcer	2
4.1 Forholdsregler i forbindelse med beskyttelse af IT-hardware og følsomme data	3
4.2 Brug af elektronisk post (e-mail)	3
4.3 Brug af netværk (herunder også trådløst) og Internetforbindelse	5
4.4 Publicering af private www-sider	5
4.5 Netcafeen/trådløst netværk	6
5. IT-afdelingens overvågning og registrering af brugernes aktiviteter	6
5.1 Formålet med IT-afdelingens overvågning og registrering af brugernes aktiviteter	6
5.2. Hvilken type oplysninger gemmer IT-afdelingen	6
5.3 I hvilke situationer registrerer og gennemgår IT-afdelingen den enkelte brugers aktiviteter	6
5.4 Hvem har adgang til at gennemgå oplysningerne om den enkelte brugers aktiviteter	7
6. Procedurer ved mistanke om misbrug af DJHs IT-ressourcer	7

1. Formål med IT-reglerne

DJH ønsker med IT-reglerne at fastlægge rammerne for opretholdelsen af et stabilt og velfungerende IT-system med et minimum af forstyrrelser af driften, samtidig med at brugernes privatliv, brevhemmelighed og personlige oplysninger søges beskyttet som foreskrevet i lovgivningen. Retningslinjerne er udstedt af højskolens ledelse i samarbejde med IT-afdelingen.

For at opretholde en optimal drift af højskolens IT-systemer og undgå diverse forstyrrelser er det nødvendigt med interne retningslinjer, der klart præciserer den gældende lovgivning i forbindelse med anvendelsen af højskolens IT-ressourcer.

Persondataloven af 1. juli 2000 kræver, at DJH, i lighed med andre virksomheder og institutioner, udformer en skriftlig information, der klart beskriver formålet med indsamling og registrering af persondata, hvis en sådan indsamling eller registrering forekommer i forbindelse med opretholdelsen af IT-systemerne. Derfor præciserer IT-reglerne også klart, hvordan og i hvilke tilfælde IT-afdelingen overvåger/inspicerer indholdet af studerende eller medarbejders e-mail eller på anden måde registrerer disses aktiviteter på eksempelvis Internettet.

Alle studerende og medarbejdere ved DJH skal gøre sig bekendt med disse retningslinjer.

2. Hvem er omfattet af IT-reglerne

Alle medarbejdere og studerende ved DJH er omfattet af IT-reglerne i de tilfælde, hvor højskolens IT-ressourcer benyttes.

3. Hvad er omfattet af IT-reglerne

IT-reglerne omfatter al benyttelse af DJHs IT-ressourcer, også i de tilfælde, hvor IT-ressourcerne benyttes til rent private formål.

Med IT-ressourcer forstås: højskolens computere, servere, fællesarkiver, mailservere, Intranet (lokalt netværk), Internetforbindelse og andet hard- og software, der er at betragte som DJHs ejendom, herunder IT-udstyr som er stillet til rådighed for medarbejdere i hjemmet.

I situationer, der falder ind under punkt 5.3 i disse retningslinjer, forbeholder DJH sig ret til at slette, flytte og inspicere data, der befinder sig på højskolens IT-ressourcer. Dette gælder således også dokumenter, arkiver, e-mails etc.

Elektronisk post (e-mails) sendt og modtaget af medarbejdere på DJH kan, i lighed med et hvert anden type dokument, i visse tilfælde være en sagsakt, hvorfor medarbejdere altid skal foretage en konkret vurdering af, om den enkelte e-mail bør gemmes og evt. videresendes til journalisering i ledelsessekretariatet, hvor der er oprettet et særskilt automatisk elektronisk arkiv.

4. Generelle regler vedr. brugen af DJHs IT-ressourcer

Både studerende og medarbejdere på DJH er forpligtet til at overholde retningslinjerne, når de benytter sig af DJHs IT-ressourcer. Du kan læse mere om højskolens IT-ressourcer på IT-afdelingens hjemmeside: <http://afdelinger.djh.dk/itafdeling/>. Her findes også links til mere information om sikkerhed, samt tips og råd vedrørende benyttelsen af højskolens IT-ressourcer. Alle studerende og medarbejdere ved DJH opfordres til at besøge ovenstående hjemmeside.

Brugernavn og password er personligt og må aldrig overdrages til andre. Ved mistanke om at brugernavn/password er kendt af andre skal IT-afdelingen kontaktes.

Generelt gælder det, at DJHs IT-ressourcer (i form af CPU-kapacitet, terminaladgang, lagerplads, netværkstrafik mv.) er begrænsede, hvorfor de udelukkende må benyttes til deres rette formål, dvs. til undervisning, forskning og arbejdsopgaver. Det er dog ligeledes tilladt at anvende højskolens IT-ressourcer til private formål, så længe dette foregår på et acceptabelt niveau og i øvrigt ikke hindrer andre brugere i at bruge udstyret til undervisning, forskning eller arbejde.

For at undgå skader på højskolens IT-udstyr og for at sikre rene og ryddelige lokaler er det ikke tilladt at spise, drikke eller ryge i computerrum, der stilles til rådighed for de studerende på DJH. Overtrædes disse ordensregler vil det medføre midlertidig eller permanent bortvisning fra de nævnte lokaler.

4.1 Forholdsregler i forbindelse med beskyttelse af IT-hardware og følsomme data

For, så vidt muligt, at forhindre tyveri af computere og deraf følgende tab og/eller spredning af følsomt datamateriale, skal DJHs medarbejdere tage følgende forholdsregler:

- **Elektronisk lås (password) på alle computere som indeholder følsomme oplysninger**
For at undgå spredning af fortroligt datamateriale som eksempelvis klagesager, detaljer om medarbejders lønforhold og lign., skal alle computere som benyttes af administrative medarbejdere forsynes med et personligt password. Andre medarbejdere, hvis computere indeholder følsomme oplysninger (evalueringer, breve, DJHs brevpapir mv.), bør også beskytte disse oplysninger ved at forsyne computeren med en elektronisk lås. Herved er det muligt at forhindre uvedkommende i at få adgang til fortroligt datamateriale, hvad enten dette forsøges i det daglige arbejde, eller i den situation hvor computeren er blevet stjålet.
- **Tag systematisk backup af data**
For at undgå at tabe vigtigt datamateriale ved tyveri eller beskadigelse af hardware, skal alle medarbejdere systematisk foretage backup af deres data. Dette kan foregå på DJHs fælles personaleserver. Ved henvendelse til IT-afdelingen udleveres det password, som er nødvendigt for at få adgang til denne server. Meningen med backup er, at datamateriale gemmes to forskellige steder. Så det er altså ikke tilstrækkeligt (eller mere sikkert), udelukkende at gemme data på DJHs fællesserver, da denne i princippet ikke er bedre sikret imod funktionsfejl end medarbejdernes egne computere (se dog næste punkt). Medarbejdere i økonomiafdelingen skal benytte afdelingens egen filserver.

Alle studerende, som bruger DJHs fællesarkiver, skal også tage sikkerhedskopi af data, for det tilfælde, at systemet skulle gå ned og data derved gå tabt.

- **Særligt følsomt materiale gemmes på fællesserveren**
Dette punkt omhandler udelukkende følsomme oplysninger fra Navision Stat samt Personaleadministrations-databasen. Materiale herfra gemmes kun på fællesserveren.
- **Frist ikke potentielle indbrudstyre ved at lade de populære bærbare computere stå frit fremme på bordene, når arbejdspladsen forlades og under hjemtransporten**

4.2 Brug af elektronisk post (e-mail)

4.2.1. Generelle regler for alle

Følgende regler gælder generelt vedrørende brugen af den af DJH tildelte e-mailkonto:

- **Tjek din postkasse med elektronisk post jævnligt (flere gange om ugen)**
Tjekkes postkassen jævnligt, er du sikker på at modtage alle vigtige oplysninger udsendt af DJH og andre via e-mail.
- **Det er ikke tilladt at "spamme", dvs. sende uopfordrede e-mails ud til en stor gruppe modtagere**
Det er ikke tilladt at anvende DJHs e-mailkonto til at chikanere andre ved brug af spam eller misbruge det elektroniske postsystem til at sende store mængder "junk mails", dvs. emails uden relevant indhold, som modtageren(e) ikke selv har indvilliget i at modtage. Du kan læse mere på [http://afdelinger.djh.dk/itafdeling/stories/storyReader\\$134](http://afdelinger.djh.dk/itafdeling/stories/storyReader$134).
- **Tjek modtagne e-mails for virus, inden du åbner eventuelle vedhæftede filer**

Brugerne har selv ansvaret for skader på egne computere og evt. tabt data i forbindelse med computervirus. Computervira optræder bl.a. i form af inficerede programmer og dokumenter. Er du i tvivl om, hvordan du tjekker vedhæftede filer for kendte vira, er du velkommen til at henvende dig til IT-afdelingen eller læse mere om emnet via IT-afdelingens hjemmeside: <http://afdelinger.djh.dk/itafdeling/>. Dog bør man altid svare "nej", hvis Microsoft Office spørger, om den må afvikle en "macro".

- **Det er ikke tilladt at påtage sig andre brugeres identitet**

Ved udsendelse af e-mails skal afsenderen altid identificere sig med korrekt navn. Af samme grund er det ikke tilladt at videregive det personlige password til DJHs e-mailsystem til andre brugere. Ved mistanke om at brugernavn/password er kendt af andre, skal IT-afdelingen kontaktes.

4.2.2. Ansatte

Fastansatte får udleveret et brugernavn og tilhørende djh.dk-mailadresse.

Alle it-ydelser på DJH's netværk er bundet til brugernavn og password.

Ansatte får udleveret en opdateret beskrivelse af ydelser ved ansættelse.

Dokumentation og manualer kan findes på www.djh.dk/manualer

Bemærk specielt afsnit 4.1, 5.2 og 5.3

Man skal være ansat på DJH i 3 måneder for at kunne få en djh.dk-mailadresse, hvilken - ud over at have Notes kalenderfunktion - giver adgang til at læse DJH-mailopslag. Alle andre kan få en mail.djh.dk-adresse (Mailport) ved henvendelse til Personaleafdelingen.

Mailportadresseindehavere kan via nærmeste leder få adgang til at læse opslag. Lederen skal kontakte Personaleafdelingen skriftligt.

Når ansættelse ophører, inddrages brugerrettighederne (herunder også e-mailadressen) omgående. Der kan, såfremt det i særlige tilfælde er absolut nødvendigt, oprettes en meddelelse på den pågældende mailadresse om, at medarbejderen er ophørt.

Det er personaleafdelingen, der opretter og sletter brugere.

4.2.3. Studerende

Studerende får udleveret et brugernavn og tilhørende mail.djh.dk-mailadresse.

Alle it-ydelser på DJH's netværk er bundet til brugernavn og password. (udleveres med e-mail-adressen).

Studerende får udleveret en opdateret beskrivelse af ydelser ved studiestart.

Dokumentation og manualer kan findes på www.djh.dk/manualer og www.djh.dk/print

Studerende kan ikke få adgang til at læse DJH-opslag uden skriftlig tilladelse fra rektor, som orienterer Personaleafdelingen om oprettelse.

Ved endt studie slettes brugerrettighederne omgående - e-mailadressen slettes tidligst efter 3 måneder.

Det er Studieadministrationen der opretter og sletter brugere.

4.2.4. CFJE

Fastansatte på CFJE har adgang til ydelsen 'Hjemmeadgang' se: www.djh.dk/hjemmeadgang

Bemærk specielt afsnit 5 til afsnit 6.

CFJE sørger selv for oprettelse af mailadresser. CFJE skal give Personaleafdelingen besked om alle oprettelser og slettede mailadresser.

CFJE's brugere og mailadresser optræder i DJH's adresseoversigt.

Adgangen til it-ydelserne sker via CFJE's lokale brugernavne og passwords. Her de brugernavne og passwords der benyttes ved CFJE's intranet-system.

4.2.5. DICAR

DICAR sørger selv for oprettelse af mailadresser. DICAR skal give Personaleafdelingen besked om alle oprettelser og slettede mailadresser.

DICAR's brugere og mailadresser optræder i DJH's adresseoversigt.

4.3 Brug af netværk (herunder også trådløst) og Internetforbindelse

Ved brug af DJHs netværk og Internetforbindelse gælder følgende regler:

- **Kopiering af programmer er ikke tilladt uden forudgående tilladelse fra IT-afdelingen**
Hovedparten af de programmer, som DJHs computere er udstyret med, er underkastet licensbestemmelser, der forbyder, at programmerne kopieres og benyttes på andre maskiner. Dette forbud mod kopiering gælder også, selvom det rent teknisk skulle være muligt at foretage en kopiering uden at bryde sikkerhedssystemet.
- **Det er ikke tilladt at forsøge at bryde sikkerhedssystemer**
Brud på sikkerhedssystemer eller forsøg på dette er strafbart, hvad enten der er tale om DJHs eller andre virksomheder eller institutioners, hvorfor dette under ingen omstændigheder må foregå fra DJHs computere eller via DJHs Internetforbindelse.
- **Det er ikke tilladt at skaffe sig adgang til data eller programmer i andre brugeres filsystemer**
Der må ikke gøres forsøg på at tilegne sig programmer eller data i andre brugeres filsystemer uden forudgående aftale med de pågældende brugere om dette. Reglen gælder også selvom det, rent teknisk, skulle være muligt at skaffe sig adgang til andre brugeres private data og programmer uden derved at bryde sikkerhedssystemet.
- **Distribution af ulovlig software eller data er ikke tilladt**
Det er ikke tilladt at distribuere eller "share" (dele med andre på Internettet) software, herunder programmer, film og mp3-filer, som du ikke selv har rettighederne til.

4.4 Publicering af private www-sider

Ved publicering af private www-sider fra DJHs server gælder følgende regler:

- **Al kommerciel anvendelse er forbudt**
Denne service må derfor udelukkende anvendes til private hjemmesider med et ikke-kommercielt sigte.
- **Indholdet af web-siderne må ikke krænke dansk lovgivning**
Indholdet må derfor eksempelvis ikke krænke de ophavsretlige regler eller indeholde personoplysninger, der ikke er tilladt i henhold til lovgivningen.
- **Alle www-sider skal være mærket med forfatterens navn og e-mailadresse**
- **Publicering af www-siderne må ikke medføre unødigt belastning af DJHs IT-ressourcer**
Ekstremt stort diskforbrug eller nettrafik må således ikke forekomme uden forudgående aftale med IT-afdelingen..

4.5 Netcafeen/trådløst netværk

Se hjemmesiden: www.djh.dk/netcafe for flere informationer om reglerne vedr. DJHs Netcafe/trådløse netværk.

Følgende regler er gældende for studerendes anvendelse af netcafeen:

- **Der er kun adgang til DJHs netværk (med egne computere) fra Netcafeen**
Det er ikke tilladt at koble egne computere på højskolens netværk uden for de nævnte områder. Overtrædes denne regel, kan IT-afdelingen inddrage netværksrettigheder uden varsel
- **Brugerne af netcafeen har selv det fulde ansvar for medbragt computer og software**
Hverken DJH eller medarbejdere i IT-afdelingen kan gøres ansvarlige for eventuelle ødelæggelser af hardware, software eller tab af data i forbindelse med benyttelse af netcafeen eller det trådløse netværk på DJH.

5. IT-afdelingens overvågning og registrering af brugernes aktiviteter

DJH og IT-afdelingen respekterer privatlivets fred, brevhemmeligheden, hemmeligholdelsen af personlige oplysninger og ophavsrettigheder i forbindelse med opretholdelsen af højskolens IT-ressourcer. I øvrigt er det DJHs opfattelse, at studerende såvel som medarbejdere som udgangspunkt respekterer og overholder de opstillede regler vedrørende brugen af højskolens IT-ressourcer. Derfor udføres der heller ikke rutineinspektioner eller andre former for rutineovervågninger af den enkelte bruger. Men, ved rutinegennemgang af IT-systemerne, kan medarbejderne i IT-afdelingen uforvarende komme i kontakt med brugernes personlige oplysninger (se også afsnit 5.4).

Som det fremgår af afsnit 5.1, 5.2, 5.3 og 5.4 forbeholder DJH sig ret til at overvåge og gennemgå den enkelte brugers aktiviteter og data, men kun i de tilfælde, hvor lovgivningen kræver det, eller hvor der er begrundet mistanke om misbrug af IT-ressourcerne.

5.1 Formålet med IT-afdelingens overvågning og registrering af brugernes aktiviteter

Af hensyn til opretholdelsen af drift, sikkerhed, og eventuel genetablering og dokumentation foretages der sikkerhedskopiering/backup af stort set alle aktiviteter, der foregår på DJHs IT-system. Hvis denne sikkerhedskopiering/backup ikke blev foretaget, kunne der opstå situationer, hvor det ville være umuligt for DJH at genetablere betydningsfulde oplysninger, dokumenter og andre former for sagsakter, som DJH er forpligtet til jf. journalpligten, samt sikre effektiv opgradering.

5.2. Hvilken type oplysninger gemmer IT-afdelingen

Alle transaktioner foretaget fra computere tilsluttet DJHs netværk logges. Transaktioner vedr. elektronisk post logges og gemmes i maksimalt en måned. Mht. transaktionerne på DJHs netværk, har IT-afdelingen mulighed for at identificere oplysninger om: 1) hvilken computer/arbejdsstation der er brugt til en given transaktion, 2) hvilken bruger, der har været logget på netværket og foretaget en given transaktion, 3) adresserne på de søgte hjemmesider, 4) dato og klokkeslæt for de foretagne søgninger. Derudover har it-afdelingen mulighed for at overvåge brugernes e-mailkonti og i yderste konsekvens inspicere indholdet af afsendte og modtagne e-mails.

5.3 I hvilke situationer registrerer og gennemgår IT-afdelingen den enkelte brugers aktiviteter

De i afsnit 5.2 nævnte oplysninger om brugernes aktiviteter der gemmes af DJHs IT-system, hører alle ind under betegnelsen "personlige data" og er derfor omfattet af Persondataloven af 1. juli 2000. Kun i ganske særlige tilfælde må DJH/medarbejdere i IT-afdelingen benytte oplysningerne om brugernes aktiviteter. De særlige tilfælde omfatter følgende situationer:

- **Når det kræves af gældende dansk lovgivning**
Eksempelvis på forlangende af dansk politi i forbindelse med efterforskningen af overtrædelser af straffeloven.

- **Hvis der eksisterer begrundet mistanke om misbrug af DJHs IT-ressourcer**
Eksempelvis chikane i form af afsendelse af "spam-mails" eller "junk-mails" i meget stor stil, jf. i øvrigt det ovenstående.
- **Ved reparation eller service af dataudstyr**
I en sådan forbindelse skal IT-afdelingen behandle oplysninger, som de måtte blive bekendt med, som fortroligt materiale, der under ingen omstændigheder må videregives eller anvendes.
- **Særlige omstændigheder**
Herunder tekniske omstændigheder, hvor en gennemgang af den enkelte brugers aktiviteter er nødvendig for at lokalisere tekniske fejl og derved opretholde driften af IT-systemet. Indbefattet under særlige omstændigheder er også situationer, hvor en gennemgang af den enkelte brugers aktiviteter er nødvendig for at undgå personskaade, tab af DJHs ejendom eller grove overtrædelser af DJHs interne retningslinjer i øvrigt.

5.4 Hvem har adgang til at gennemgå oplysningerne om den enkelte brugers aktiviteter

Som hovedregel er det udelukkende medarbejderne i DJHs IT-afdeling, som har adgang til disse oplysninger med henblik på fejlfinding og opretholdelse af højskolens IT-systemer. Medarbejderne i IT-afdelingen har strenge pålæg om ikke at forfølge brugernes personlige aktiviteter uden at have et klart og sagligt grundlag for at gøre dette. Hvis IT-medarbejderne under den normale vedligeholdelse af IT-ressourcerne uforvarende kommer i kontakt med personlige oplysninger, som f.eks. en brugers private e-mails, er det ikke tilladt IT-medarbejderne at læse eller på anden måde gøre sig bekendt med indholdet af en sådan e-mail. I tilfælde med grove eller gentagne brud på de opstillede retningslinjer i denne IT-politik kan DJHs ledelse gives adgang til oplysningerne med henblik på en endelig vurdering af de studiemæssige/tjenstlige konsekvenser heraf (se også afsnit 6. vedrørende procedurerne ved mistanke om overtrædelser af reglerne vedr. DJHs IT-ressourcer).

I alle tilfælde, hvor en gennemgang af en brugers aktiviteter skønnes at være nødvendig, skal brugeren forinden informeres herom. Undtaget fra denne regel er særlige tilfælde, hvor det ikke umiddelbart er muligt at komme i kontakt med den pågældende bruger, og hensynet til opretholdelsen af IT-systemets drift klart overskygger hensynet til den enkelte bruger.

6. Procedurer ved mistanke om misbrug af DJHs IT-ressourcer

Overtrædes de opstillede regler for brugen af DJHs IT-ressourcer vil den enkelte bruger i første omgang modtage en henstilling fra IT-afdelingen om for fremtiden at følge det opstillede regelsæt.

I alvorligere tilfælde med grove eller gentagne forsøg på misbrug af DJHs IT-ressourcer, kan IT-afdelingen lukke for brugerens adgang til e-mail-systemet/netværket og efterfølgende foretage indberetning om misbruget/mistanken herom til DJHs ledelse.

Særligt grove overtrædelser af de opstillede regler kan i sidste ende resultere i bortvisning af de studerende fra DJH (læs mere her: [http://afdelinger.djh.dk/studienaevn/stories/storyReader\\$31](http://afdelinger.djh.dk/studienaevn/stories/storyReader$31)) og få tjenstlige konsekvenser for medarbejderne.