

24.05.12

IT-Politik

Retningslinjer og regler
for medarbejderes
og elevers brug af
IT-faciliteter hos
Mentiqa Odense



Skolen for børn med særlige forudsætninger



Indhold

Formål	3
IT-faciliteter	4
Gode råd til brugernes om IT-sikkerhed	5
Generelle IT-regler for medarbejdere	7
Retningslinjer for medarbejderes brug af e-mail	8
Adgang til og brug af hjemmesiden	10
Adgang til brugernes personlige data og dokumenter	10
Retningslinjer for elever og gæster	11
Hvad er uacceptabel brug af IT-faciliteter?	12
Hvordan håndteres mistanke om uacceptabel brug af IT-faciliteter?	14



Formål

Formålet med IT-politikken er:

- Beskrive de retningslinjer og regler der gælder for medarbejderes og elevers brug af Mentiqa Odenses IT-faciliteter, herunder regler for arbejdsrelateret og privat brug af mailsystemer.
- At henvise til gældende lovgivning *) på området.
- At sikre at retningslinjer og regler på området er aftalt og kommunikeret.

Mentiqa Odenses IT-politik er baseret på en grundlæggende tillid til at medarbejdere og elever udviser personlig ansvarlighed i brugen af vores IT-faciliteter, og at hver enkelt bruger gør sig bekendt med vores IT-politik og gældende lovgivning på området *).

IT-politikken beskriver også, hvad der sker, når det i enkeltsager skal afklares om IT-politikens retningslinjer og regler ikke er overholdt.

*)

Persondataloven:

<http://www.datatilsynet.dk/lovgivning/persondataloven>

Offentlighedsloven:

<https://www.retsinformation.dk/Forms/R0710.aspx?id=59474>

Forvaltningsloven:

<https://www.retsinformation.dk/Forms/R0710.aspx?id=105127>

Lov om ophavsret:

<https://www.retsinformation.dk/forms/r0710.aspx?id=129901>

Om IT-strategiske spørgsmål

For god ordens skyld skal det præciseres, at nærværende IT-politik ikke beskriver forretnings- og uddannelsesspecifikke strategier og målsætninger på IT-området.

IT-politikken omhandler alene de generelle og lovgivningsrelaterede rammer for medarbejderes og elevers brug af Mentiqa Odenses IT-faciliteter.



IT-faciliteter

Hvilke IT-faciliteter er omfattet af IT-politikken?

- Internt datanetværk, der binder alle lokationer i Mentiqa Odense sammen, herunder trådløs adgang på alle lokationer.
- Adgang til internet.
- Windows PC'ere (stationære og bærbare) og tilhørende udstyr.
- Fastnettelefoner og mobiltelefoner/smartphones/PDA'ere.
- Netværksprintere.
- Skolens hjemmeside.
- Fælles- og personlige drev på netværket – herunder fjernadgang hertil.
- Standard Office programpakke - inkl. Outlook mail- og kalenderprogram samt WebMail.
- Fagsystemer, bl.a.:
 - Journal-, sags- og dokumenthåndteringssystemer
 - Økonomisystem (Summasummarum)
 - Bibliotekssystem (udlånssystem af undervisningsmaterialer).
 - Hjemmesidesystem/CMS (Joomla)
 - Publicering på nettet, herunder evt. personlige arbejds/studierelaterede hjemmesider, pædagogiske logbøger, portfolios, blogs, wikies o.lign.



Gode råd til brugerne om IT-sikkerhed

IT-sikkerhed bliver du først opmærksom på, når det ER gået galt - når du sletter dokumentet ved et uheld, eller computeren bliver lukket ned af en virus, mens du har allermest travlt.

IT-sikkerhed er også dit ansvar!

1. Brug din sunde fornuft når du bruger IT – det kan redde dig fra mange ærgrelser og spildt arbejdstid. Det stærkeste kort i beskyttelsen af din computer og dine vigtige dokumenter er din sunde fornuft - så du behøver ikke at være ekspert!
2. Stop aldrig din PC's antivirussystem.

Adgangskode

3. Brug en sikker adgangskode. Adgangskoden er den vigtigste beskyttelse mod misbrug af dine data og din person - vælg den med omhu – og få lavet den om ved mistanke om at den er kommet tredjepart i hænde..
4. Vær varsom med din pc. Den er en mulig adgangsvej til alle Mentiqa Odenses systemer og data. Forlad aldrig din PC uden at logge ud af systemet og låse skærmen. Selv den bedste adgangskode er nytteløs, hvis du går fra din maskine uden at logge ud.
5. Udlevér aldrig din adgangskode til andre - den er strengt personlig. Lad aldrig Windows eller andre programmer huske dine adgangskoder. En god adgangskode indeholder mindst 8 tegn og er en blanding af tal og bogstaver - brug ikke æ, ø og å.

E-mails

6. Håndter e-mails og vedhæftede filer med omtanke. E-mails kan indeholde vedhæftede filer, du ikke bør åbne eller se på. Sund skepsis er dit bedste forsvar.
7. Sørg for at din e-post jævnligt efterses for ny post, og slet evt. spam-mails.

Internet

8. Brug Internet med omtanke. Din adfærd på nettet efterlader mange spor. Materiale, du henter, kan være beskyttet af ophavsret eller indeholde data der er skadelige for din computer.

Dokumenter

9. Gem dine dokumenter på netværkets fællesdrev og/eller dit personlige drev. Når din PC ikke er koblet til Mentiqa Odenses netværk, så husk at gemme kopier af vigtige dokumenter på en USB-nøgle eller en ekstern harddisk - så du har en sikkerhedskopi at falde tilbage på ved et uheld. Gem dine dokumenter flere steder, så er du mindre sårbar.
10. Hvis du er i tvivl om IT-sikkerhed så kontakt Mentiqa Odenses IT Administrator.



IT-sikkerhed – i øvrigt

For at IT-sikkerheden kan opretholdes, er det væsentligt, at alle følger de givne retningslinjer og er opmærksom på, at brud på sikkerheden et enkelt sted kan have følger for mange. IT-systemer, der ejes af Mentiqa Odense, skal være tilgængelige for institutionen. Det betyder at, systembrugernavne og tilhørende kodeord, krypteringsnøgler og nøgler til andre sikringsmekanismer, skal deponeres i pengeskabe eller på anden betryggende vis, således at administrator eller andre bemyndigede medarbejdere i givet fald kan få adgang til systemerne, ved den normale systemansvarliges fravær. De deponerede oplysninger skal ajourføres, når der sker ændringer. Materiale, der er omfattet af offentlighedsloven eller forvaltningsloven, må ikke opbevares/arkiveres på krypteret form.

Kryptering og efterfølgende dekryptering, der sker (automatisk) mellem afsender og modtager for at sikre datatransporten er ikke omfattet af forbudet mod kryptering.

Husk om sikkerhedskopiering!

Brugernes personlige dokumenter gemt lokalt på PC'en er IKKE omfattet af IT-afdelingens Sikkerhedskopiering bortset fra administrationsserveren. Sørg derfor for at dine personlige dokumenter også gemmes på dit personlige drev på netværket, hvor IT-afdelingen sørger for daglig sikkerhedskopiering/backup.



Generelle IT-regler for medarbejdere

Ved at anvende Mentiqa Odenses IT-faciliteter accepterer alle brugere at opfylde gældende love, herunder nærværende retningslinjer og regler, samt evt. lokale bestemmelser. Alle brugere er ansvarlige for enhver brug af deres personlige adgange og konti og har pligt til at håndtere passwords mv. forsvarligt, således at de ikke utilsigtet kommer andre i hænde. Brugere må ikke beskadige, fjerne eller ændre mærkater (fx PC-navn, modelnummer, serienummer, stregkoder) på Mentiqa Odenses IT-udstyr.

Privat brug

IT-faciliteter på Mentiqa Odense understøtter institutionens drift. Det er tilladt i begrænset omfang, at IT-faciliteterne anvendes til privat brug, forudsat at den private brug fortrinsvis sker udenfor normal arbejdstid og at den ikke forstyrrer eller overbelaster IT-driften. Brug af fildelingssystemer er ikke tilladt!

IT-udstyr hjemlånt af medarbejdere er omfattet af nærværende IT-politik.

Dokumentformat ved brug af OpenOffice og Office2007-pakken

I forbindelse med brugen af Office2007 og OpenOffice skal alle brugere gemme Office-dokumenter i formatet "97-2003 dokumentformat", fx Word: *.doc og Excel: *.xls., af hensyn til kompatibilitet med tidligere og eksterne systemer.

Brug af udstyr, herunder installation af programmer

Mentiqa Odenses PC'ere (og printere/kopimaskiner), er konfigureret til vores netværk, og vedligeholdes automatisk via netværket, herunder sikkerhedsopdateringer af Windows, Office-pakken og anden software eller opdateres af IT-administratoren.

Af hensyn til en effektiv og sikker drift er det alene IT-administratoren der må ændre disse indstillinger, ligesom udstyret alene må serviceres og repareres af IT-administratoren (med undtagelse af kopimaskinerne der serviceres af eksternt firma).

Brugerne må gerne installere andre programmer til egen arbejdsmæssig brug efter aftale med IT-administratoren, men det påhviler alene brugeren at sikre at licensregler og trediepartsrettigheder overholdes for disse programmer.

IT-administratoren hjælper gerne med installation af programmer, både shareware-programmer og licensbaserede programmer.



Retningslinjer for medarbejderes brug af e-mail

! Ang. retningslinjer for behandling af indgående e-post refereres til Mentiqa Odenses administrative procedure.

E-mail

- E-mails har status som al anden skriftlig kommunikation på Mentiqa Odense.
- Der må til arbejdsrelaterede opgaver ikke benyttes andre e-mail adresser end de af Mentiqa Odense tildelte e-mail adresser. Der oprettes dog i reglen ikke e-mail adresser til time ansatte.
- Du kan give en kollega adgangsrettigheder til at tilgå din postkasse i tilfælde af længerevarende fravær. Pågældende medarbejder/kollega er underlagt fortrolighed og tavshedspligt overfor din mail.
- Lederen kan, hvis det findes nødvendigt i forbindelse med en opgaves udførelse, beslutte at du skal give en kollega adgangsrettigheder til at tilgå din postkasse. Pågældende medarbejder/kollega er underlagt fortrolighed og tavshedspligt overfor dine e-mails.
- Det er ikke tilladt at have automatisk viderestilling fra egen mailadresse/mailboks til mailsystemer udenfor Mentiqa Odenses e-mail system.
- Du skal være opmærksom på, at forskellige typer bilag (vedhæftede filer) kan indeholde virus. Åbn derfor ikke bilag hvor du er usikker på indholdet. Kontakt eventuelt IT-administratoren, hvis du er i tvivl.
- Hvis du modtager post, der er adresseret forkert, skal du sende svar til afsenderen om at posten er adresseret forkert.
- Svar ALDRIG! på spam mails.

Besvarelse af e-mails:

!

Retningslinjer for besvarelse af e-mail fra elever fastlægges i personalehåndbogen. Svartider for interne og eksterne henvendelser kan være yderligere fastlagt af lokale servicemål for ekspedition af henvendelser. Hovedprincippet er at du skal sørge for at de e-mails du modtager bliver besvaret i løbet af få arbejdsdage – af dig, en kollega eller en anden medarbejder hos Mentiqa Odense.



Besvarelsen kan f.eks. alene være en bekræftelse af modtagelsen og, hvis henvendelsen fx kræver igangsættelse af en egentlig sagsbehandling, en angivelse af forventet ekspeditionstid.

I øvrigt:

- Check din mailboks for modtagne e-mails hver arbejdsdag, så vidt det er muligt.
- Besvar e-mails senest 3 arbejdsdage efter modtagelsen – evt. med en meddelelse der angiver hvornår der vil blive svaret på henvendelsen, og hvis det ikke er dig selv der besvarer den, hvem der så vil besvare henvendelsen.
- Hvis du ikke kan efterse indbakken i din mailboks i en periode, så sørg for at en kollega passer den i denne periode, eller bed IT-administratoren indstil din mailboks til at sende et autosvar til afsenderen med besked om:
 - hvornår du besvarer e-mails igen, og
 - hvem der kan kontaktes i stedet, eller at e-mailen automatisk bliver videresendt til en kollega som vil besvare henvendelsen.

Kodeks for indhold i e-mails

- Skriv altid et emne i emnerubrikken, og skriv høfligt, kort, præcist, enkelt og overskueligt.
- Husk at anvende en signatur der tydeligt angiver dine kontaktinformationer for modtageren.
- Brug Cc (kopi til – modtagere angivet hér kan ses af de andre modtagere) med omtanke. Pas på med at svare alle oprindelige modtagere hvor dette ikke aftalt – det er ofte ikke nødvendigt.
- Brug Bcc (blind kopi til – modtagere angivet hér kan ikke ses af de andre modtagere) når der skal skrives til flere adressater samtidigt, udenfor skolen, som f.eks. forældre.
- Brug ikke e-mail til følelsesladede budskaber.
- Husk at e-mails skal kunne tåle at blive læst af andre. Nogle medarbejdere har brug for (evt. i perioder) at give en sekretær eller en anden kollega adgang til sin mailboks.
- Husk at dine e-mails i tilfælde af mistanke om (evt. andres) IT-misbrug kan blive åbnet af ledelsen ved undersøgelser af mistanken.

Adgang til brugernes mailkonti

Hvis det af driftsmæssige årsager er nødvendigt, kan IT-administratoren uden forudgående varsel åbne en medarbejders mailkonto for at udbedre problemet. Mailkontoens ejer skal hurtigst muligt orienteres herom og have anvisning på korrekt anvendelse af systemet.

IT-administratoren er pålagt fortrolighed og tavshedspligt i forbindelse med tilgang til mailkonti.

Adgang til og brug af hjemmesiden

Adgangskoder udleveret til at tilgå Mentiqa Odenses hjemmeside må ikke videregives til tredjepart, og udskiftes af IT-administratoren med passende mellemrum.

Hovedprincippet for adgang til hjemmesiden er:

- Forældre og elever har kun læserettigheder.
- Lærerne har redigeringsrettigheder til lektiesider hvor de løbende indtaster lektier der er givet for.
- Bestyrelse, skoleleder og sekretær har redigeringsrettigheder til hele hjemmesiden.

Adgang til brugernes personlige data og dokumenter

Ved driftsarbejde kan IT-administratoren have behov for at tilgå data og filer i forbindelse med vedligeholdelse eller undersøgelse. IT-administratoren er pålagt fortrolighed og tavshedspligt i forbindelse med tilgang til disse personlige data og filer.

Overvågning og logning af vores IT-systemer sker alene af hensyn til drift, fejlretning, sikkerhed, genetablering og dokumentation. Det kan fx være i forbindelse med undersøgelse af it-faciliteters logfiler for fejl og/eller driftsforstyrrelser, netværksovervågning, undersøgelse af e-post der ikke er blevet leveret til en postkasse, håndtering af virus- og spamfiltre, brug af internet, afklaring af ressourcebegrænsninger o.lign.

Adgang til logning og overvågning er begrænset til personale hvis opgave det er at sikre IT-driften. IT-medarbejdere (og evt. eksterne IT-konsulenter) skal respektere fortrolighed og tavshedspligt, brugernes personlige og evt. private data og filer, og skal behandle disse i overensstemmelse med bestemmelserne i persondataloven.

Håndtering af brugerdata og brugerrettigheder

IT-administratoren opretter de basale brugerdata på Mentiqa Odense IT systemer.

Brugernavne/bruger-ID, adgangskoder og mail-adresser vælges i samarbejde mellem brugeren og IT-administratoren, eller eksempelvis for UNI-C's vedkommende, skolens sekretær.

Brugeres adgang til IT-faciliteterne styres i en vis udstrækning via tildeling af brugerrettigheder. Disse rettigheder skal løbende revideres i overensstemmelse med brugerens behov.

En brugers adgang til IT-faciliteter skal lukkes hvis brugeren ikke længere er ansat, er sygemeldt på ubestemt tid, har længerevarende orlov eller andre begrundede forhold, hvor ledelsen vurderer at adgangen bør lukkes.

!

Ledelsen og administrationen kan udarbejde procedurer, herunder tidsfrister, for ændring af medarbejders og elevernes adgang til IT-faciliteter og IT-systemer ved tilgang, afgang og flytning.



Retningslinjer for elever og gæster

Du kan bruge Mentiqa Odenses IT-faciliteter ved at koble din egen PC til vores netværk, eller ved at bruge en af vores PC-arbejdspladser.

Som bruger af Mentiqa Odenses IT-faciliteter har du følgende forpligtigelser:

- Såfremt du er i besiddelse af eget personligt brugernavn og adgangskode, skal du altid koble dig på Mentiqa Odenses netværk med det. Brugernavn og adgangskode må ikke gives eller udlånes til andre.
- Du skal altid logge af PC'en, når du forlader den.
- Du må ikke foretage ulovlige handlinger ved brug af Mentiqa Odenses IT-faciliteter og internettet. *F.eks. er download af musikfiler, video og andet beskyttet materiale forbudt, ligesom kopiering og distribution af piratkopier ikke må finde sted.*
- Du må ikke foretage handlinger ved brug af Mentiqa Odenses IT-faciliteter, der er til skade for Mentiqa Odenses omdømme.
- Du må ikke ændre computerens opsætning og/eller installere programmer på computeren, medmindre det sker som led i undervisningen eller efter aftale med den IT-ansvarlige.
- Du må ikke anvende Mentiqa Odenses computere i kommercielt øjemed.
- Ved overtrædelse udsætter du dig for følgende:
- Du kan få din ret til at anvende Mentiqa Odenses computere inddraget.
- Du kan i særlig grove tilfælde blive bortvist fra Mentiqa Odense og/eller blive politianmeldt. *Du risikerer at få bøde eller i særlig grove tilfælde fængselsstraf som følge af ulovlige handlinger foretaget ved brug af Mentiqa Odenses computere. Erstatningsansvaret påhviler alene den enkelte bruger, der har foretaget den ulovlige handling. Mentiqa Odense er ikke ansvarlig for ikke-ansattes (dvs. elevers) handlinger.*

Adgang til brugernes data, filer og mails

Ved driftsmæssige forstyrrelser og ved begrundet mistanke om alvorligt misbrug af Mentiqa Odenses computere, kan IT-administratoren efter forudgående godkendelse hos ledelsen, foretage gennemgang af en brugers data og filer, herunder evt. mail, og iværksætte undersøgelser.

Den enkelte bruger skal i givet tilfælde orienteres snarest muligt efterfølgende.

IT-administratoren er pålagt fortrolighed og tavshedspligt i forbindelse med tilgang til personlige data, filer og e-mails.



Hvad er uacceptabel brug af IT-faciliteter?

Uacceptabel brug af Mentiqa Odenses IT-faciliteter er brug der:

- er direkte ulovlig,
- kompromitterer IT-sikkerheden, eller
- skaber IT-driftforstyrrelser ved brud på retningslinjer eller regler.

Eksempler

Nedenfor gives en række eksempler på aktiviteter, der må anses for uacceptable. Listen er ikke udtømmende.

Det er uacceptabelt for brugere, der ikke er autoriseret hertil, at:

- Forsøge at få adgang til personlige og/eller personfølsomme informationer.
- Anvende en anden brugers adgangskode(r).
- Søge informationer om password eller data som tilhører andre brugere.
- Udføre aktiviteter, som ikke overholder gældende love og regulativer, herunder uautoriseret kopiering af ophavsretsligt materiale, brug af retsbeskyttet software uden licens eller formidling af uautoriserede kopier af retsbeskyttet software til andre.
- Forsøge at omgå IT-sikkerhedsmetoder og operativsystemer eller undersøge sårbarheder i andre IT-faciliteter eller på netværk.
- Anvende Mentiqa Odenses IT-faciliteter til privat kommerciel brug.
- Opfange eller undersøge data uden de fornødne rettigheder eller autorisation.
- Forstyrre eller afbryde andre brugeres og IT-faciliteters arbejde eller deltage i en aktivitet, som kan medføre tab af andre brugeres og IT-faciliteters data.
- Publicere indhold på personlige arbejdsrelaterede hjemmesider der kan kompromittere Mentiqa Odense eller er ulovlig.
- Udføre aktiviteter som kompromitterer Mentiqa Odenses IT-sikkerhedsregler og retningslinjer eller andre lokale politikker, herunder forsøg på at omgå IT-sikkerhedsbestemmelser eller ressourcebegrænsninger ved at tilsløre eller forfalske sin identitet.

Brug af Internet

- Det er ikke tilladt at anvende internetadgangen til private kommercielle formål.
- Brug af internet fra Mentiqa Odenses netværk bør ske med omtanke da infektion med virus eller anden skadelig software kan få store negative konsekvenser for hele netværket.
- Hold dig fortrinsvis til internetsider fra kendte firmaer eller organisationer, og søg ikke efter "useriøse" sider. Der kan ikke gives en fast definition på hvad "useriøse" sider er, men et pejlemærke er en sund fornuft og undgåelse af sider med porno, spil, chat, hacker,



musik, video, fildeling og lignende. Udover at søgning på nogle af disse typer hjemmesider kan være ulovlig, er det ofte på denne type sider, at der gemmer sig virus, spyware og ødelæggende programmer.

- Download fra internettet må kun foretages, hvis det har et arbejds- eller undervisningsmæssigt formål.
- Vær opmærksom på, at al færden på internettet efterlader elektroniske spor, der kan henføres til Mentiqa Odense, på de servere der er besøgt. Når du færdes på internettet fra Mentiqa Odenses netværk bør du derfor aldrig besøge sider eller foretage handlinger, der på nogen måde kan virke kompromitterende for Mentiqa Odense.
- Vær opmærksom på, at det ikke er lovligt at publicere fx fotos på nettet af personer der ikke forudgående har givet tilladelser hertil, ligesom loven om ophavsret naturligvis skal respekteres ved publicering og tilgængeliggørelse af andres værker via nettet.



Hvordan håndteres mistanke om uacceptabel brug af IT-faciliteter?

I tilfælde hvor der kan konstateres en overtrædelse af Mentiqa Odenses IT-politik, eller hvor der er en begrundet mistanke om overtrædelse af Mentiqa Odenses IT-politik, skal IT-administratoren kontaktes. Henvendelser om overtrædelser af Mentiqa Odenses IT-politik skal altid undersøges og behandles seriøst, og henvendelsen skal besvares. Den mistænkte leder og IT-administratoren skal i alle tilfælde orienteres. Enhver kendt overtrædelse af Mentiqa Odenses IT-politik skal analyseres for at udelukke eventuelle forsætlige fejl. Den mistænkte, dennes leder og IT-administratoren inddrages i undersøgelsen. Det vil i mange tilfælde være tilstrækkeligt at afklare en hændelse ved en opklarende samtale med de implicerede parter. Det kan dreje sig om misforståelser, tekniske fejl eller brugerfejl og dermed være uforsætlige for brugeren af den pågældende IT-facilitet.

En anden kilde til undersøgelse af påstande om uacceptabel brug af Mentiqa Odenses IT-faciliteter er:

- Logfiler, idet en del af it-brugen i Mentiqa Odense logges, og dermed kan efterspores og henføres til en given bruger.
- IT-administratoren kan om nødvendigt og ved tvivlsspørgsmål vælge at inddrage eksterne konsulenter eller andre myndigheder.

Alle personer involveret i opklarende virksomhed eller overvågning er undergivet tavshedspligt vedrørende de oplysninger af fortrolig karakter, de måtte få kendskab til.

Ledelsen behandler eventuelle sanktioner i forbindelse med overtrædelsen af Mentiqa Odenses IT-politik efter gældende regler på Mentiqa Odense, herunder de personaleretslige regler.

Ulovlig brug af Mentiqa Odenses IT-faciliteter (herunder internet), kan desuden medføre påtale, skriftlig advarsel og have disciplinære konsekvenser som fx afskedigelse i henhold til gældende regler.

I særligt grove tilfælde kan ledelsen foretage en politianmeldelse og inddrage politiet i efterforskningen. Pressen vil i givet tilfælde blive håndteret af skolens leder.

Overtrædelser af Mentiqa Odenses IT-politik af ekstern part - herunder misbrug af IT-faciliteter vil om nødvendigt blive anmeldt til CERT (Computer Emergency Response Team).

Vedrørende undersøgelse af påstande om uacceptabel brug af Mentiqa Odenses IT-faciliteter henvises endvidere til Dansk IT's "Quick guide – Optimering af efterforskningsmulighederne ved datakriminalitet", der kan downloades her:

http://dit.dk/Nyt_fra_DIT/Presse/~media/Files/Publikationer/Gratis_publikationer/quick_guide_endelig_lav.as hx



Ovennævnte IT-politik er vedtaget af Bestyrelsen for Mentiqa Odense d. 24/5 2012