



---

# It-politik

For studerende på Erhvervsakademi Aarhus

---

## Indhold

Formål med it-politikken .....	2
Gyldighedsområde .....	2
Generelle regler.....	2
De ti bud om sikker it-brug .....	3
Uacceptabel brug af it-faciliteter og overvågning .....	4
Administration af brugerkonti .....	4
Adgang til brugernes personlige mailkonti, data og dokumenter .....	5
Overvågning og logning af it-systemer.....	5
Videoovervågning .....	6
Brug af udstyr, herunder installation af programmer .....	7
Misbrug.....	7
Digital dannelse er et fælles ansvar .....	7
Brug af udlåns pc'er .....	8
Tyveri .....	8
Mail .....	8
Ved uacceptabel brug af it-faciliteter.....	9
Lovgivning .....	9

## Formål med it-politikken

---

Erhvervsakademiets kultur er baseret på kvalitet, åbenhed og ansvarlighed. Det gælder også it-tilbud og -systemer til de studerende.

It-politikken bidrager til sikker it-drift, og udgangspunktet er tillid til, at it-brugerne sætter sig ind i it-politikken, som præsenteres her, og udviser sund fornuft og ansvarlighed i brugen af vores it-faciliteter.

## Gyldighedsområde

---

It-politikken omfatter brugen af alle akademiets it-faciliteter, herunder:

- Alle netværksbaserede it-faciliteter og it-systemer
- Personligt it-udstyr udlånt af akademiet
- Privat it-udstyr, der kobles på akademiets it-faciliteter

It-politikken gælder for alle studerende og kursister på Erhvervsakademi Aarhus.

## Generelle regler

---

Ved at anvende akademiets it-faciliteter accepterer du at opfylde gældende love, herunder nærværende retningslinjer og regler, og at du vil anvende vores it-systemer på en professionel, ansvarlig og hensynsfuld måde - kun til undervisningsmæssige formål.

Alle brugere er ansvarlige for enhver brug af deres personlige rettigheder og konti. Alle brugere har pligt til at håndtere passwords mv. forsvarligt, således at de ikke utilsigtet kommer andre i hænde.

Brugerne må ikke beskadige, fjerne eller ændre mærkater (fx pc-navn, modelnummer, serienummer, stregkoder) på akademiets it-udstyr.

## De ti bud om sikker it-brug

---

Du skal følge de ti bud ved enhver brug af it og internet fra akademiets netværk, da virus, hacking eller skadelig software kan få alvorlige konsekvenser for netværket og risikere at påvirke hele akademiets drift.

1. Åbn aldrig "mistænkelige" filer, dvs. filer, hvor du er i tvivl om, hvad det er, eller hvem afsender er.
2. Svar/klik aldrig på noget i phishing-mails (mails med det formål at franarre dig adgangskoder, kontooplysninger og lignende).
3. Brug sikre adgangskoder, dvs. med både store og små bogstaver samt tal og gerne specialtegn – og giv dem aldrig til andre.
4. Beskyt alle dine "devices" (også tablets, mobiltelefoner o.l.) med password og/eller pinkode/fingerprint, og genbrug ikke password
5. Undgå, at andre bruger dit udstyr ved altid at låse din computer (fx via Windows + L eller Control + Shift + Power på en Mac), når du forlader den.
6. Vær kritisk, når du installerer apps på din telefon eller tablet og software på din computer.
7. Hold din pc opdateret og husk altid at have et opdateret antivirusprogram installeret på den. Er du i tvivl, kan du kontakte it-Servicedesk for vejledning. Har du mistanke om, at din PC er inficeret med virus, kan du søge hjælp hos it-Servicedesk.
8. Brug altid din skolemail ved kommunikation med Erhvervsakademi Aarhus. Det er din skolemail eller e-Boks, vi benytter, når vi skal kontakte dig.
9. Tilgå ikke sider med porno eller spil. Søgning på den type sider kan være ulovlig, og her gemmer sig tit virus, spyware og ødelæggende programmer.
10. Husk at indrapportere sikkerhedshændelser til it-Servicedesk eller din underviser - også hvis du har mistanke om, at uvedkommende har adgang til din konto eller dit it-udstyr.

## Uacceptabel brug af it-faciliteter og overvågning

---

Ved uacceptabel brug af akademiets it-faciliteter forstås brug, der:

- Er direkte ulovlig
- Kompromitterer it-sikkerheden
- Skaber it-driftsforstyrrelser ved brud på politikker/retningslinjer.

Nedenfor finder du en række eksempler på aktiviteter, der ikke er tilladt, når du bruger akademiets internetadgang:

- Anvendelse af internetadgangen til private kommercielle formål
- Anvendelsen af en anden brugers adgangskode
- Søgning af informationer om password eller data, som tilhører andre brugere.
- Aktiviteter, som ikke overholder gældende love, herunder uautoriseret kopiering af ophavsretsligt materiale, brug af licensbeskyttet software uden licens eller formidling af uautoriserede kopier af licensbeskyttet software til andre
- Forsøg på at opfange eller undersøge data uden de fornødne rettigheder eller autorisation.

Vær opmærksom på, at al færden på internettet efterlader elektroniske spor og kan spores. Mange steder kan du foretage valg om brug af kun nødvendige cookies. Hvis det er muligt, benyt færrest mulige cookies.

Bruger du akademiets udstyr/netværk, kan de elektroniske spor henføres til Erhvervsakademi Aarhus (og efterfølgende til dig).

Når du færdes på internettet fra akademiets netværk, bør du derfor aldrig besøge sider eller foretage handlinger, der på nogen måde kan virke kompromitterende for akademiet.

## Administration af brugerkonti

---

Studerende oprettes som brugere på akademiets it-systemer på basis af brugerdata, som oprettes af akademiets studieadministration. Brugernavn, password og mailadresse oplyses i brugererklæringen samt hvordan brugeren selv skal ændre sit password.

Ved afslutning af uddannelsen deaktiveres den studerendes brugerkonto på første dag efter uddannelsens ophør. 90 dage senere slettes den studerendes brugerkonto og tilhørende data.

Brugeres adgang til it-faciliteterne styres via tildeling af brugerrettigheder, primært på grundlag af informationer fra det studieadministrative system.

En brugers adgang til it-faciliteter lukkes, hvis:

- Brugeren ikke længere er studerende
- Brugeren har længerevarende orlov
- Der er andre begrundede forhold, hvor ledelsen vurderer, at adgangen bør lukkes.

## Adgang til brugernes personlige mailkonti, data og dokumenter

---

Hvis der er driftsmæssige problemer, kan det blive nødvendigt, at it-medarbejdere – uden forudgående varsel – åbner en studerendes mailkonto for at udbedre problemet. Mailkontoens ejer vil hurtigst muligt blive orienteret herom og få anvisning på korrekt anvendelse af systemet.

Ved driftsarbejde kan it-medarbejdere have behov for at tilgå data og filer i forbindelse med vedligeholdelse eller undersøgelse.

It-medarbejdere er pålagt fortrolighed og tavshedspligt i forbindelse med tilgang til mailkonti, de netop omtalte personlige data og filer.

## Overvågning og logning af it-systemer

---

Overvågning og logning af vores it-systemer sker alene af hensyn til drift, fejlretning, sikkerhed, genetablering, markedsføring 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, indsigtsager o.l.

Da akademiet skal være i stand til at overholde en række lovgivningskrav i forhold til bl.a. persondataforordningen, straffeloven, forvaltnings- og offentlighedsloven skal akademiet afveje en række forhold:

På den ene side - skal akademiet, på lige fod med andre offentlige institutioner, være i stand til at kunne behandle indsigtssager i forhold til persondataforordningen og aktindsigtssager i forhold til forvaltnings- og offentlighedsloven.

På den anden side - er akademiet i lige så høj grad interesseret i **ikke** at krænke vores studerendes ret til privatliv. Hvis du undtagelsesvist afsender eller modtager privatrelateret indhold på din skolemail (Outlook), bør du placere al mail med privatrelateret indhold i mappen mærket "Privat". Det samme bør du gøre med privat indhold på dit OneDrive og H-drev.

Adgang til logning og overvågning er begrænset til personale, hvis opgave det er at sikre it-driften. Ledelsen har således kun adgang til data fra logning/overvågning ved mistanke om misbrug eller kriminalitet.

It-medarbejdere og evt. eksterne it-konsulenter respekterer fortrolighed og har tavshedspligt i forbindelse med tilgang til brugernes mailkonti, personlige og evt. private data og filer, og behandler disse i overensstemmelse med bestemmelserne i persondataloven.

## **Videoovervågning**

---

Akademiet foretager videoovervågning af udvalgte områder som fx indgangspartier og visse gangområder. Formålet er dels at skabe øget tryghed for studerende og medarbejdere ved at forebygge kriminalitet som tyveri, overfald, vold og lignende, dels at forbedre mulighederne for at opklare kriminalitet.

Alle optagelser fra videoovervågningen opbevares på en sikker og forsvarlig måde, og vil kun blive gennemset i tilfælde af kriminalitet. Optagelserne må ikke offentliggøres, videregives eller forevises til andre end politiet. Optagelserne slettes automatisk efter ti arbejdsdage, medmindre der er begrundet mistanke om kriminelle forhold.

## Brug af udstyr, herunder installation af programmer

---

Akademiets AV-udstyr (f.eks. Clevertouch skærme og Airtames), printere og udlåns-pc'er er konfigureret til vores netværk og vedligeholdes automatisk via netværket, herunder sikkerhedsopdateringer af Windows, Office-pakken og anden software.

Af hensyn til en effektiv og sikker drift er det alene it-afdelingen, der må ændre disse indstillinger, ligesom det udelukkende er it-afdelingen, der må servicere og reparere akademiets udstyr.

## Misbrug

---

Hvis du har mistanke om, at dit password er blevet misbrugt, eller at andre har fået kendskab til det, skal it-Servicedesk informeres med det samme, der så vil nulstille adgangskoden.

**Hvis it-Servicedesk får mistanke om misbrug af din konto bliver dit password ligeledes nulstillet. Desuden bliver den konkrete sag anmeldt som et sikkerhedsbrud til skolens GDPR-ansvarlige og du vil blive underrettet.**

Skift password på: <https://mobil.efif.dk/Login.aspx>

## Digital dannelse er et fælles ansvar

---

Mobning, chikane, krænkelser, deling af billeder uden samtykke via sociale medier samt alle former for hacking, svindel med billetter og handel via digitale medier er absolut forbudt. Erhvervsakademi Aarhus har et stort fokus på, at de studerende kan begå sig sikkert og moralsk i alle situationer, og det er vigtigt at passe på sig selv. I bedes være varsomme ved bl.a. forespørgsler fra ukendte, eller hvis I modtager tvivlsomme links.

Det er en kriminel handling at dele andres billeder/videoer, hvis de ikke har givet samtykke - og det gælder selvfølgelig også billeder/videoer af seksuel karakter.



## Brug af udlåns pc'er

---

Som udgangspunkt skal du selv medbringe din egen pc. Ved særlige lejligheder er det dog muligt at låne pc'er af skolen. Brugerne må ikke ændre i program- og systemopsætninger på pc'erne. it-afdelingen vil sørge for rutinemæssigt at nedlæse og ajourføre programmer på pc'erne, så pc'ernes funktionalitet er intakt. Alle data på pc'ernes harddiske vil blive slettet. Ønsker du at gemme dine data skal det ske på dit personlige drev, i skyen eller på USB-drev. Når du er færdig med at arbejde med pc'en, skal du logge dig ud og slukke pc'en.

## Tyveri

---

Vær opmærksom på, at opbevaring af egen pc sker på eget ansvar. Lad ikke din pc ligge uden opsyn. Skolen dækker ikke for tyveri af pc på skolens lokaliteter.

## Mail

---

Du får tildelt en skole e-mailadresse, når du påbegynder dit studie. E-mails er at betragte som personlig post, og du må ikke åbne andres e-mail uden deres samtykke.

Svar aldrig på spam-mail og phishing-mail.

Al korrespondance, der ikke er markeret som privat i emnefeltet, eller som ikke ligger i en "Privat"-mappe, er formelt set at betragte som akademiets ejendom, hvorved andre i princippet kan få adgang til at læse dem.

Du skal undgå at benytte din skolemail til privat brug (f.eks. i forbindelse med sociale medier (fx Facebook), chat, debatfora og nyhedsgrupper på internettet samt helt private modtagere). Dette skyldes dels, at afsenderadressen bliver forbundet med Erhvervsakademi Aarhus, dels at risikoen for at blive ramt af spammails og sikkerhedsmæssige angreb øges i takt med, at e-mailadressen oplyses til parter, man ikke kender.

## Ved uacceptabel brug af it-faciliteter

---

I tilfælde, hvor det konstateres, at akademiets it-politik overtrædes, eller hvor der er begrundet mistanke om overtrædelse, skal it-chefen kontaktes.

It-chefen har ansvaret for sagens videre forløb.

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 overtrædelser, hvor brugeren ganske uforsætligt har overtrådt reglerne.

Hvis der er tale om forsætlige overtrædelser af akademiets it-politik (og altså ikke simple fejltagelser), vil den mistænkte, dennes nærmeste uddannelsesleder og rektor/prorektor blive inddraget i undersøgelsen sammen med it-chefen.

Ulovlig brug af akademiets it-faciliteter (herunder internet) kan medføre påtale, skriftlig advarsel og have disciplinære konsekvenser som fx bortvisning i kortere eller længere perioder eller permanent og i yderste konsekvens politianmeldelse.

## Lovgivning

---

Lovgivning, der relaterer sig til it-politikken:

- Databeskyttelsesloven
- Forvaltningsloven
- Offentlighedsloven
- Lov om ophavsret
- TV-overvågningsloven.

Januar 2022

Hanne Troels Jensen  
forsknings- og it-chef