

I N F O R M A T I O N M E D O M T A N K E

**INFORMATIONSSIKKERHED
I KØGE KOMMUNE**



KØGE KOMMUNE

INDHOLD

Information med omtanke	3
Din pc	4
Adgangskode	5
Virus	6
E-mail og sikkerhed	7
Medarbejdersignatur	8
Tavshedspligt	8
Sikkerhedskopiering	8
Log	8
Internettet	9
Print	9
Dine bærbare enheder	10
Samtykke	11
Håndtering af personoplysninger	12
Alle hændelser skal indberettes	15
Gode vaner	16
Kontakt	17

INFORMATION MED OMTANKE

Som medarbejder i Køge Kommune har du ansvar for at passe på borgernes og kommunens data. Det er derfor en vigtig del af dit job at kende og overholde reglerne for informationssikkerhed.

*Pjecen her er et uddrag af kommunens samlede informationssikkerhedspolitik, **som du kan læse på Kjukken**. Den giver et overblik over de overordnede regler. Du vil sikkert støde på spørgsmål i forhold til dit specifikke arbejdsområde. Disse skal afklares med din leder.*

Helt overordnet handler det om at passe på personoplysninger og kunne dokumentere brugen af dem. Derfor:

- *Indsaml kun den nødvendige data*
- *Brug fagsystemer og blanketter*
- *Slet/makuler efter brug.*

Du er altid velkommen til at kontakte informations-sikkerhedskoordinatoren, hvis du har spørgsmål om informationssikkerhed. Se kontaktinformation på sidste side.

Venlig hilsen

*Peter Frost
Kommunaldirektør*

D I N P C

Når du først er logget på, må du ikke overlade din pc til andre - hverken kolleger eller udefrakommende.

Husk altid at låse it-udstyr, mobil og pc (⌘ + L), hvis du forlader det. Så er du helt sikker på, at ingen andre kan tilgå dit indhold.

Hvis du har mistanke om misbrug eller andre sikkerhedsbrud, skal du informere informationssikkerhedskoordinator og - om muligt - stoppe hændelsen med det samme. Kontakt Servicedesk, hvis du har brug for teknisk hjælp.

Du må udelukkende bruge IT-systemerne i forbindelse med dit arbejde. Det er dog tilladt i begrænset omfang at anvende e-mail, internet og Officepakken til privat brug.

Udtjent IT-udstyr skal altid afleveres til IT-afdelingen, som sørger for at slette data, før udstyret kasseres eller gives videre.

A d g a n g s k o d e

Når du bliver oprettet som IT-bruger i Køge Kommune, får du udleveret et brugernavn og en engangskode. Første gang du logger på kommunens netværk, skal du ændre din adgangskode til en personlig kode. Brugernavn og adgangskode er personlige og må kun bruges af dig.

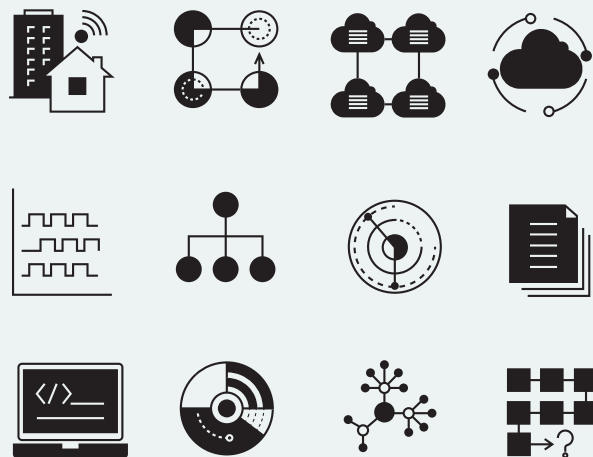
På Kjukken kan du finde retningslinjerne for adgangskoder og vejledning i at udarbejde stærke koder.

Du kan beholde din adgangskode i op til tre år.

Hvis du har mistanke om, at andre kender eller har brugt din adgangskode, skal du straks ændre den og herefter indberette til informationssikkerhedskoordinator. Hvis du har glemt din adgangskode, kan du få en ny af Servicedesken.

Værd at vide om adgangskoder

- Oplys ikke din adgangskode til andre.
- Skriv ikke din adgangskode på en seddel eller i en e-mail.
- En god adgangskode er en bogstavs- og talkombination, som er nem for dig at huske.
- Din adgangskode skal bestå af 10-16 tegn, store og små bogstaver, tal og tegn.
- Du skal omgås din kode på samme måde, som du omgås din kode til dit dankort.



Virus

Der er installeret antivirusprogrammer på alle kommunens pc'er, men der kommer hele tiden nye vira. Beskyt både din egen pc og Køge Kommunes IT-systemer:

- Hvis du har mistanke om, at din pc har fået en virus, så kontakt Servicedesk med det samme.
- Der må ikke sidde en diskette, cd-rom eller UBS-nøgle i pc'en, når du tænder den.
- Vær særlig opmærksom, når du åbner e-mail - også vedhæftede filer, da de kan indeholde virus. Pas især på filer med underlige eller lokkende navne. Også selv om de kommer fra nogen, du kender.
- Videre send IKKE virusadvarsler. Kontakt i stedet Servicedesk, som vil vurdere, om varslet er en reel trussel.
- Download kun filer fra sider på internettet, som du har tillid til.
- Du må gerne downloade og installere programmer efter aftale med din leder. **På Kjukken kan du læse om programmer, du selv må installere.** Er du i tvivl, kan du kontakte Servicedesk.

E-mail og sikkerhed

E-mail må i begrænset omfang anvendes til privat brug. Når du skal sende personoplysninger eller fortrolige oplysninger til borgere eller eksterne samarbejdspartnere, skal du sikre dig, at det altid foregår krypteret. Fx med Doc2Mail eller 'Send digitalt' i Outlook. Almindelig afsendelse af mails fra Outlook er ikke sikker til personoplysninger eller fortrolige oplysninger.

Personoplysninger må ligge i din postkasse, så længe det er relevant for en konkret arbejdsopgave. Dog aldrig mere end 30 dage.

Du må ikke bruge automatisk videresendelse af e-mail fra din postkasse.

Køge Kommune registrerer din brug af e-mail. Ved mistanke om ulovlig brug af e-mail kan ledelsen i samarbejde med IT-afdelingen åbne og læse al e-mail og eventuelle vedhæftede filer.

E-mail med følsomme data

Hvis du ønsker at sende følsomme oplysninger til eksempelvis en borger, skal du sende dem via sikre systemer, fx 'Send digitalt i Outlook' eller Doc2Mail. Du må aldrig sende en almindelig e-mail med personoplysninger. Heller ikke selv om en borger har givet dig lov til det.

Medarbejdersignatur

Har du en NemID-medarbejdersignatur, skal den beskyttes på samme måde som din adgangskode. Signaturen er personlig og må kun bruges af dig. Kontakt Servicedesk, hvis du har mistanke om, at den bliver misbrugt.

Din NemID-medarbejdersignatur må ikke benyttes til private formål.

Tavshedspligt

Som medarbejder i Køge Kommune har du tavshedspligt. Fortrolige informationer må under ingen omstændigheder deles med uvedkommende – hverken under eller efter ansættelse.

Sikkerhedskopiering

Der bliver løbende taget sikkerhedskopier af al information på kommunens servere. Husk derfor altid at gemme de dokumenter, regneark og andre filer, du arbejder med, i eDoc eller på et netværksdrev. De er ikke sikret på computerens skrivebord.

Log

Al behandling og opbevaring af personoplysninger skal kunne dokumenteres. Derfor logges alle adgange og handlinger, der involverer personoplysninger – og loggen bliver kontrolleret, bl.a. ved stikprøver.

Internettet

Internettet er et vigtigt arbejdsredskab og skal betragtes som et sådant. Alle IT-brugere har derfor adgang til internettet. Internettet må i begrænset omfang anvendes til privat brug.

Dit brug af internettet registreres centralt.

- Tal altid med din leder, hvis du har brug for nye programmer.
- Tryk ikke på links, du ikke har tillid til.
- Du må ikke pådrage kommunen udgifter, ansvar eller skade i forbindelse med brug af internettet.
- Du skal være påpasselig med at opgive din e-mailadresse på internettet. Den kan blive anvendt til spam.
- Besøg ikke hjemmesider af yderliggående, underlødige eller pornografisk karakter. De er ofte årsag til vira.
- Vær opmærksom på, at du ikke må dele arbejdsdokumenter med kolleger eller samarbejdspartnere via sociale medier, som fx Facebook, LinkedIn, Twitter og diverse blogs. Lovgivningen for disse tjenester er ofte forskellig fra den danske med hensyn til ophavsret.

Print

Personoplysninger på print skal skærmes mod uvedkommende og makuleres eller i en af de aflåste papircontainere efter brug. Skal de gemmes, skal de opbevares forsvarligt, så uvedkommende ikke kan komme til dem.

Du må gerne have et stykke papir med personoplysninger med dig, men du skal passe godt på det og destruere det efter brug.

DINE BÆRBARE ENHEDER

Køge Kommunes bærbare enheder - fx bærbare pc'er, pda'er, USB-nøgler, mobiltelefoner m.fl. - bruges ofte uden for kommunens bygninger. Det stiller særlige krav til både den fysiske sikkerhed og til sikkerheden af de data, der opbevares på dem. Derfor er der nogle enkle regler, du skal følge:

- Efterlad aldrig bærbare enheder uden opsyn.
- Arbejder du med fortrolige oplysninger i det offentlige rum, skal du sikre dig, at ingen kan se med.
- Bærbare pc'er må kun bruges af en medarbejder, der er autoriseret som bruger.
- Du må ikke ændre udstyrets sikkerhedsindstillinger, opsætning eller antivirusberedskab.
- Opbevar kun nødvendige data på udstyret. Sørg for at rydde op og slette data jævnligt.
- Når du gemmer dine oplysninger på centrale servere og systemer, er data sikret, og du er automatisk sikret backup, så du ikke mister informationer, selv om udstyret skulle gå i stykker eller forsvinde.

USB-nøgler

USB-nøgler må gerne bruges til datatransport eller lignende, hvis de er krypterede. **Se hvordan du sikrer dig det på Kjukken.**

Husk at slette data, straks behovet for transport eller opbevaring er ophørt (max 30 dage).



Samtykke

Som offentlig myndighed er der ikke krav om samtykke, når det drejer sig om indsamling og behandling af oplysninger, der er nødvendige for at udføre en lovmæssig opgave. Men skal du lave opgaver uden for de lovmæssige opgaver, skal der indhentes samtykke.

Et samtykket skal blandt andet indeholde oplysninger om, hvem der indhenter det, formålet, hvor længe data gemmes og klare instrukser om, hvordan samtykket kan trækkes tilbage.

Har du brug for at indhente et samtykke, kan du finde blanketter på Kjukken under '**Værktøjer og vejledninger**'.

HÅNDTERING AF PERSON- OPLYSNINGER

Personligoplysninger er enhver form for information, der helt eller delvist kan føres tilbage til en person.

Eksempler på almindelige personoplysninger

- væsentlige sociale problemer
- andre rent private forhold
- økonomi
- skat
- gæld
- sygedage
- tjenstlige forhold
- familieforhold
- bolig
- bil
- eksamen
- ansøgning og cv
- ansættelsesdato
- stilling
- arbejdsområde
- arbejdstelefon
- navn
- adresse
- fødselsdato



Jo mere følsomme oplysningerne er – eller jo flere der behandles – jo større krav er der til behandling af dem. Hvis du er i tvivl, så spørg din leder til råds.

Følsomme personoplysninger

- race
- etnisk oprindelse
- politisk, religiøs eller filosofisk overbevisning
- fagforeningsmæssige tilhørsforhold
- genetiske data
- biometriske data med henblik på entydig identifikation
- helbredsoplysninger
- seksuelle forhold eller orientering

Personoplysninger skal behandles og opbevares sikkert

Brug altid fagsystemer til personoplysninger, som fx eDoc, Vitae, OPUS osv.

Fagsystemer sikrer:

- personlige oplysninger og dit arbejde, hvis du skulle miste din pc, bliver angrebet af virus og malware eller hacket af datakriminelle.
- at du automatisk overholder loven i forhold til at beskytte personoplysninger korrekt.
- at der tages backup af data. Der bliver fx ikke taget sikkerhedskopier af data på de enkelte pc'er.

Du skal bruge de systemer, der er bestemt inden for dit specifikke område. Mangler du systemer eller procedurer, skal du give din leder besked, så der kan findes en løsning.

Midlertidig opbevaring

Du må gerne have oplysninger liggende uden for sikre systemer under en konkret arbejdsopgave. Dog aldrig mere end 30 dage.

Hvis du gemmer uden for sikre systemer, mens du løser en opgave, skal det være på krypterede enheder (computer, USB-nøgle, mobiltelefoner eller lignende) - og du skal passe særligt godt på dem.

Du må aldrig gemme personoplysninger på andre systemer end dem, der er godkendt af kommunen, brug fx ikke sociale medier eller Dropbox.

Husk

Alle personoplysninger skal beskyttes mod utilsigtet eksponering, både kolleger imellem og over for borgere.

Du må kun søge de informationer, du skal bruge til en given opgave, og du må ikke dele dem med uvedkommende.

Alle hændelser skal indberettes

Alle hændelser skal indberettes til informationssikkerhedskoordinatoren, og de skal - om muligt - stoppes med det samme. Det gælder også, hvis der er mistanke om misbrug eller strafbare forhold.

En hændelse kan dække over mange ting, fx:

- Mistanke om svagheder.
- Brud på fortrolighed, integritet og tilgængelighed
- Brud på fysisk sikkerhed
- Manglende efterlevelse af politikker eller procedurer
- Forsøg på at omgå sikkerheden i systemer – også selv om hensigten har været god
- Malware, virus eller hacking
- Driftsforstyrrelser (systemændringer, hardwarefejl mm.)

Udstilles og kompromitteres personoplysninger har kommunen pligt til at informere Datatilsynet og de berørte personer. Du skal derfor straks informere din leder. **Læs mere på Kjukken**, hvor der ligger en procedure for, hvordan du skal forholde dig.

GODE VANER

- Indsaml kun de personoplysninger, der er nødvendige for at løse din opgave.
- Gem ikke mere end højst nødvendigt.
- Slet alt, der ikke bliver brugt.
- Gem altid personoplysninger i fagsystemer. Så er data beskyttet, sikret backup og kan dokumenteres.
- Gem kun personoplysninger midlertidigt uden for fagsystemer, fx dit personlige netværksdrev, krypteret USB osv., og flyt dem til et sikkert system hurtigst muligt (max 30 dage).
- Det er IKKE tilladt at opbevare fortrolige eller følsomme oplysninger på ukrypterede USB-nøgler og tilsvarende bærbare enheder.
- Du må ikke skaffe dig oplysninger om personer, medmindre du skal bruge dem til et arbejdsrelateret formål.
- Personoplysninger på print skal skærmes mod uvedkommende og opbevares forsvarligt, så uvedkommende ikke kan komme til dem.

KONTAKT

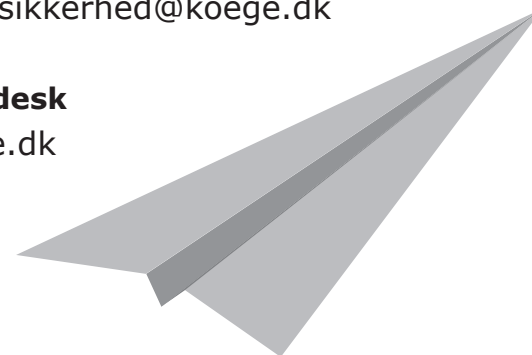
Informationssikkerhedskoordinator

informationssikkerhed@koege.dk

IT's Servicedesk

2082@koege.dk

5667 2082



Vi har alle et **ansvar** for at passe på borger-
nes og kommunens data.

Det er derfor en vigtig del af jobbet at passe
på informationer og **overholde informations-
sikkerhedsreglerne.**