

For at beskytte data og informationer mod tab og for at sikre borgerne størst mulig retssikkerhed skal alle ansatte følge kommunens it-sikkerhedspolitik samt reglerne i persondataforordningen.

TAVSHEDSPLIGT

Som medarbejder i Albertslund kommune har du tavshedspligt. De personfølsomme og fortrolige oplysninger du får kendskab til gennem dit arbejde, må ikke uberettiget videregives til andre eller komme til uvedkommendes kendskab. Det gælder både under og efter din ansættelse.

LÅS DIN PC NÅR DU FORLADER DEN

Aktiver altid pauseskærmen (Windows-tasten + L) når du forlader PC'en eller klik på ikonet "Gå til møde" på skrivebordet.

BÆRBARE, TABLETS og MOBILTELEFONER

Efterlad ikke din bærbare, mobiltelefon eller andet mobilt it-udstyr uden opsyn på offentlige steder. Sæt altid kode på mobiltelefoner og tablets.

ADGANGSKODER

Du må aldrig videregive dine personlige adgangskoder til andre.

Du må aldrig benytte andres konti og password.

Hvis du har mistanke om, at din adgangskode er blevet kendt af andre, skal du straks skifte den. Har du mistanke om, at adgangskoden er blevet misbrugt, skal du straks kontakte IT-Support på tlf. 43 68 60 60.

INTERNETTET

Du må ikke bruge sociale netværkstjenester (Facebook f.eks) til at udveksle fortrolige oplysninger om borgere eller kommunens forhold.

Al din færden på internettet skal kunne rummes indenfor dansk lovgivning.

Al brug af internettet bliver automatisk logget. Din færden på internettet bliver dermed registreret, og vil kunne spores.

Du må kun downloade dokumenter fra kendte kilder.

Brugere må ikke, helt eller delvist, kopiere, downloade bøger, artikler, rapporter eller andre dokumenter medmindre dette specifikt tillades fra rettighedshaveren.

Du må aldrig downloade programmer uden godkendelse fra rettighedshaveren.

Privat brug af internettet er tilladt i begrænset omfang, hvis arbejdet tillader det.

VIRUS, PHISHING OG SUSPEKTE HJEMMESIDER

Kommunens it-udstyr er beskyttet mod virus, spam m.v..

Modtager du alligevel en mistænkelig mail, så slet den, **sva**r aldrig på den og åbn aldrig vedhæftede filer eller links i disse mistænkelige mails. Besøg heller ikke suspekte hjemmesider og brug altid din sunde fornuft og omtanke.

E-MAIL

Journaliser alle emails, der indgår som relevante led i sagsbehandling og benyt ikke Outlook som arkiv.

Det er dit ansvar, at din indbakke bliver tømt jævnligt.

Ved planlagt fravær skal du sørge for at aktivere dit autosvar via "ikke tilstede-assistent" i Outlook

Undgå så vidt muligt masseudsendelser. Skal et dokument sendes til mange anbefales det at det sker ved link til Teams eller SBSYS.

E-mails skal anvendes med betænksomhed, da medarbejderen via afsenderadressen fremstår som repræsentant for Albertslund kommune, uanset om indholdet måtte være af privat karakter.

SIKKER POST

Når du skal kommunikere med en borger via email, og dialogen vedrører personfølsomme oplysninger, skal du benytte Digital post på borger.dk. Hvis borgeren ikke har oprettet en

digital postkasse på borger.dk skal du kommunikere via brev.

Når du skal kommunikere med offentlige eller private virksomheder via e-mail vedr. personfølsomme oplysninger, skal du benytte de sikre postkasser. Se vejledningen på intranettet under "Digitalisering og IT".

Du behøver ikke at benytte de sikre postkasser for at sende personfølsomme oplysninger til andre ansatte kommunen da denne kommunikation foregår i kommunens netværk. Husk at slette disse mails 30 dage efter endt sagsbehandling.

GEM DATA OG DOKUMENTER FORSVARLIGT

Du skal altid opbevare data:

- I SBSYS
- I lokale fagsystemer
- På kommunens ONEDRIVE

Du må ikke:

Brug Onedrive til lagring af personfølsomme oplysninger. Brug OneDrive til dokumenter som indgår i sagsbehandlingen eller interne dokumenter i deres endelige form. Hvis du på et tidspunkt *ikke* har adgang til dit fagsystem kan du godt benytte OneDrive til at gemme Worddokumenter som en midlertidig løsning. Her må du **kun** gemme personfølsomme oplysninger i **maksimum 30 dage**.

DATATYPER

1 og 2 er fortrolige

1. Følsomme eller fortrolige personoplysninger om borgere og ansatte i Albertslund kommune.
F.eks.: Helbred, race, religion, seksualitet, politisk tilhørsforhold, sociale problemer, strafbare forhold cpr-nr. mv.
2. Værdioplysninger er oplysninger med væsentlig betydning for kommunen. Det er f.eks.:
Udbudsmateriale, kontrakter, budgetter, it-infrastruktur og dokumentationsmateriale.

3 og 4 skal behandles med omtanke

3. Almindelige personoplysninger: Oplysninger, der identificerer en person. F.eks. Navn, adresse, e-mail, telefonnumre m.v.
4. Kommunens interne oplysninger: Er data som kun er tænkt brugt internt i kommunen
F.eks. vagtplaner eller interne notater.

MATERIALE PÅ INTERNETTET

Hvis du publicerer materiale på internettet, skal du være særlig omhyggelig med hvad der offentliggøres.

Er du i tvivl om. Hvordan data skal behandles, så spørg din nærmeste leder.

OPSLAG I IT-SYSTEMER

Du må kun slå op i it-systemer, hvis det er i forbindelse med dine egne arbejdsopgaver. Alt, hvad der sker på kommunens it-systemer, kan løbende blive registreret. Det sker af hensyn til Albertslund kommunes drift og sikkerhed.

IT-SIKKERHED INFORMATIONSSIKKERHED SIKKER ADFÆRD PÅ INTERNETTET

I Albertslund Kommune har vi alle et ansvar for at passe på borgernes og kommunens data.

I denne pjece finder du de vigtigste råd og regler om it-sikkerhed og god og sikker adfærd på internettet.



Albertslund Kommune