Greve Kommune

# Informations-sikkerhed i Greve Kommune

En samlet vejledning til
medarbejdere i Greve kommune.

Greve Kommune

# Indhold

# Indledning

Som kommune har vi ansvaret for at behandle borgere, ansatte, virksomheder, foreninger, politikere og samarbejdspartneres informationer trygt og sikkert, ligesom vi har ansvaret for at informationerne er tilgængelige, når de skal bruges.

Hvis de oplysninger vi har er forkerte eller vi ikke kan stole på dem, er der risiko for, at vi ikke kan løse vores opgaver på en måde der lever op til databeskyttelsesreglerne.

Det stiller en række krav til dig som medarbejder i Greve Kommune. Du skal vide, hvordan vi i vores daglige arbejde sikrer informationer og beskytter mod at havne i forkerte hænder, mod virus- og hackerangreb, afluring og misbrug med videre.

Du skal desuden være bevidst om kun at bruge de informationer, du arbejdsmæssigt har behov for og sikre dig, at informationerne altid er beskyttet i henhold til deres følsomhed.

Kravet om sikker anvendelse af data omfatter alle ansatte, konsulenter, elever, kommunalpolitikere og andre, der får adgang til kommunens data.

I denne folder finder du generelle råd og regler for sikker anvendelse af data og informationer i Greve Kommune.

# På arbejdspladsen

Du får udleveret et personligt bruger-id og et password for at få adgang til Greve Kommunes systemer og data. Bruger-id'et skal sikre, at det er dig, der er logget på systemerne, og at der sker en registrering af, hvem der har læst eller arbejdet med data. Måske får du også et medarbejdercertifikat, som er tilknyttet dit bruger-id.

**Du skal…**

Lave et godt password, som består af en kombination af bogstaver, tal/tegn samt små og store bogstaver og som er på minimum 12 tegn.

Låse din skærm, når du forlader din pc, også selv om det er for en kort periode (Windows + L).

Være særligt opmærksom, hvis du arbejder et sted, hvor der er offentlig adgang til din arbejdsplads og skærmskifte dit password med det samme, hvis du tror, at nogen kan have set dit password.

**Du må ikke…**

Bruge dit unikke Greve Kommune password i andre sammenhænge.

Nedskrive dit password.

Bruge personlige oplysninger såsom fødselsdage, familienavne, postnumre og lignende til dit password.

Bruge ord, som er fundet i ordbøger til dit password.

Deaktivere sikkerhedsindstillinger på din pc, for eksempel fjerne den automatiske skærmlås eller slå antivirusprogrammet fra.

Bruge dit medarbejdercertifikat til private formål.

# Hvis du arbejder med persondata

Persondata er alle oplysninger, som kan føres tilbage til en person, eksempelvis cpr-nummer, navn, adresse, e-mailadresse med videre Brug kun oplysninger, som er relevante for det arbejde, du skal udføre. Alle opslag logges, og der foretages stikprøver med jævne mellemrum.

**Du skal…**

Være omhyggelig med at sikre, at uvedkommende ikke får adgang til følsomme eller fortrolige oplysninger.

Gemme persondata i relevante fagsystemer eller journalsystem.

**Du må…**

Udveksle persondata internt med dine kolleger, hvis det er nødvendigt og lovligt i forhold til de arbejdsopgaver, I udfører.

Gemme persondata på fildrev eller mail i højst 30 dage. Herefter skal data enten lægges ind i fagsystem eller slettes.

**Du må ikke…**

Skaffe dig oplysninger om personer, eksempelvis familie og venner, hvis du ikke skal bruge det i dit arbejde.

Lagre personoplysninger på fildrev, usb-drev eller lignende som fast arbejdsgang.

Opbevare eller behandle fortrolige eller følsomme oplysninger på privat udstyr.

Indsamle persondata, der ikke er et lovmæssigt grundlag for at indsamle.

Videregive persondata, medmindre der er et lovmæssigt grundlag for det, og at borgeren er oplyst om, at det sker.

Anvende usb-drev til at opbevare følsomme eller fortrolige personoplysninger.

# Brug af mail

'Sikker mail', er krypterede forsendelser, som sikrer, at mails kan sendes sikkert via internettet.

**Du skal…**

Bruge 'Send digitalt"', eller sende via et fagsystem, hvis du sender en mail med følsomme oplysninger til modtagere uden for kommunen.

Sikre dig, at modtagere af følsomme oplysninger kan modtage dem sikkert.

Være kritisk, når der kommer mails fra en ukendt afsender eller mails med underligt indhold fra kendte afsendere - f.eks. med opfordring til at klikke på et link i mailen, da klik på links kan medføre virus.

Løbende arkivere relevante mails i ESDH-systemet og slette mails med følsomme eller fortrolige personoplysninger fra postkassen inden 30 dage.

**Du må…**

Sende og modtage mails med følsomme eller fortrolige oplysninger, så længe det sker internt, det vil sige via greve.dk adresser.

Sende, modtage og besvare mails med følsomme oplysninger til eksterne modtagere, hvis du sender dem som "Send digitalt".

**Du må ikke…**

Åbne mails med mistænkeligt indhold eller klikke på links, som du er i tvivl om.

Viderestille din arbejdsmail til din private mailadresse.

Videresende mails med følsomme eller fortrolige oplysninger til din private mail.

Bruge din arbejdsmail til private formål.

# Virus

**Du skal…**

Kontakte din brugerinstruktør straks, hvis du har mistanke om, at din pc har fået virus.

Sørge for at der bliver indberettet et sikkerhedsbrud til sikkerhedsbrud@greve.dk, hvis der er en mulighed for, at din pc har fået virus.

Kontakte din brugerinstruktør, hvis du har mistanke om, at antivirusprogrammet ikke virker.

**Du må ikke…**

Slå pc'ens sikkerhedsforanstaltninger, såsom antivirus software, skærmlås og lignende, fra.

# Internet

**Du skal…**

Anvende internettet med omtanke og undgå sider, der kan være stødende eller krænkende eller potentielt kan indeholde malware.

Være klar over, at alt, hvad du foretager dig via internettet, logges, og vil kunne føres tilbage til Greve Kommune og dig.

Overholde kommunens program- og licensregler og kun downloade software, som er godkendt af IT-afdelingen.

Sikre dig at materiale, du uploader til internettet, ikke indeholder fortrolige eller følsomme oplysninger.

**Du må…**

Benytte internettet i privat øjemed i begrænset omfang.

Downloade software, som er godkendt af IT-afdelingen.

**Du må ikke…**

Søge efter eller besøge sites, som indeholder porno, hacking, krænkende adfærd eller ulovligt materiale om eksempelvis terror, vold med videre.

Ulovligt download af materiale, som andre har ophavsretten til, herunder musik, film, spil, programmer og visse former for publikationer og lignende.

# Sociale netværk

Sociale netværk kan være Facebook, Twitter, Instagram og lignende Kommunen har oprettet en række officielle sider, hvor det er muligt at kommunikere med borgerne. Siderne faciliteres af kommunens kommunikationsteam, som løbende overvåger og fjerner anstødeligt indhold.

**Du skal…**

Tænke over dit ordvalg og overveje, hvad du skriver om din arbejdsplads.

Være klar over, at der er forhold, som er omfattet af tavshedspligt og at denne også gælder efter din ansættelses ophør.

Være klar over, at journalister gerne må citere fra private profiler på sociale medier.

Være klar over, at internettet aldrig ”glemmer”, så det kan være nærmest umuligt at få slettet uheldige billeder, historier eller ytringer.

**Du må…**

Deltage i offentlige debatter, så længe dine indlæg ikke er i strid med tavshedspligten, og det fremgår tydeligt, at dine indlæg er et udtryk for din personlige holdning og ikke nødvendigvis er i overensstemmelse med Greve Kommunes officielle politik.

Deltage i diverse erhvervsrettede fora (med arbejdsmail), hvis det har faglig relevans.

**Du må ikke…**

Bruge din arbejdsmail og dit password til private sociale profiler.

Lægge billeder ud af andre, medmindre du har fået deres accept.

Skrive injurierende eller krænkende indhold.

Dele borgernes persondata på sociale medier, ej heller hvis det er i arbejdssammenhæng.

# Bærbart udstyr og flytbare medier

Bærbart udstyr dækker over bærbare pc'er, smartphones og tablets. Flytbare medier kan være usb-enheder, eksterne harddiske, hukommelseskort og lignende.

**Du skal…**

Medbringe dit bærbare udstyr som håndbagage, hvis du har udstyret med på rejse.

Være opmærksom på, hvem der kan kigge med, når du arbejder på rejsen.

Være opmærksom på, at mobile hotspots/offentlige trådløse forbindelser kan være usikre, og at du kan risikere, at dit password bliver afluret.

Skifte dit password, hvis du har mistanke om, at det kan være blevet afluret.

Kryptere følsomme eller fortrolige oplysninger, der opbevares på udstyr under transport.

Straks kontakte din brugerinstruktør, hvis dit udstyr er bortkommet eller stjålet.

Aflevere defekt udstyr til IT, som sørger for sikker destruktion.

**Du må ikke…**

Efterlade dit bærbare udstyr uden at låse skærmen.

Lade familiemedlemmer bruge dit bærbære udstyr.

Efterlade bærbart udstyr eller flytbare medier uden opsyn, medmindre de er forsvarligt låst inde.

Gemme følsomme eller fortrolige oplysninger på bærbart udstyr, medmindre det er sikret med passende sikkerhedsforanstaltninger (kryptering, sikker logo og lignende).

Tage kasseret udstyr med hjem.

Bruge flytbare medier (usb-enheder og lignende) på kommunens udstyr.

# Fysisk sikkerhed

Fysisk sikkerhed omfatter personers færden, udstyr, døre, vinduer, overvågning, alarmer, papirarkiver og lignende.

**Du skal…**

Være opmærksom på gæsters og borgeres færden, således at ikke-ansatte eskorteres, hvis de har ærinde på kontorer, printerrum eller andre steder, hvor der kan være følsomme oplysninger.

Sørge for, at papirdokumenter med følsomme og fortrolige oplysninger makuleres eller smides i aflåste containere til formålet efter endt brug.

Være opmærksom på, hvad du taler om i det offentlige rum.

Sørge for at fjerne følsomme eller fortrolige dokumenter fra skrivebordet og låse dem inde ved arbejdstids ophør, eller når du forlader kontoret.

Lukke vinduer og døre, når du forlader kontoret.

**Du må ikke…**

Lade gæster være alene på kontorer eller i printerrum.

Smide dokumenter med fortrolige eller følsomme oplysninger i almindelige papirkurve eller skraldespande.

# Rapportering af sikkerhedsbrud

Et sikkerhedsbrud kan være en hændelse, hvor der sker en utilsigtet eller ulovlig ødelæggelse, tab, ændring eller videregivelse af persondata som behandles elektronisk. Eksempler kan være identitetstyveri, mails til forkerte borgere, lån af en anden kollegas bruger-id, bortkommet udstyr med videre

I tilfælde af sikkerhedsbrud skal du straks kontakte din brugerinstruktør og straks indberette hændelsen på intranettet (Vores Greve) under ”Sikkerhedsbrud”.

# Informationssikkerhedspolitik, GDPR og kontaktpersoner

Alle brugere, der har adgang til Greve Kommunes informationer, skal sætte sig ind i Greve Kommunes Informationssikkerhedspolitik, vores principper for databeskyttelse og tilhørende relevante vejledninger og procedurer.

Herudover skal man i det daglige, som bruger, altid følge de anvisninger der bliver givet af ledelse eller brugerinstruktører, således det sikres at man behandler data på den mest hensigtsmæssige måde.

Ved spørgsmål vedrørende Informationssikkerhed eller GDPR bør du i første omgang tage fat i din brugerinstruktør. Din leder vil altid vide hvem din brugerinstruktør er.