Databeskyttelse - er en del af vores DNA

Informationssikkerhed er også dit ansvar

-Pas på din computer

-Pas på borgernes data

-Styrk sikkerheden, når du danner, sender og gemmer data om elever og forældre.

Informationssikkerhed er en del af din hverdag

Indhold

Hvorfor Informationssikkerhed?

Velfungerende it og adgang til nødvendig information er en forudsætning for, at vi kan løse vores opgaver i folkeskolen effektivt. Vi skal i fællesskab sørge for at beskytte borgernes data og vores systemer bedst muligt.

Du er som it-bruger en vigtig medspiller til at sikre kommunens it-systemer og data. I denne folder finder du et kort rids af kommunens retningslinjer for Informationssikkerhed samt gældende lovgivning.

Denne folder er udarbejdet af Børne- og Uddannelsesforvaltningen (BUF) og bygger på retningslinjer og informationer fra Køge Kommunes "Information med omtanke"

Hvilket ansvar har jeg som medarbejder?

Du skal som medarbejder og it-bruger følge de retningslinjer, der er beskrevet i denne folder. Det er dit ansvar at overholde retningslinjerne, og det er vigtigt, at du løbende på Dokken holder dig orienteret om de gældende retningslinjer.

Din nærmeste leder vil informere om nye tiltag eller ændringer i forhold til informationssikkerheden i skolevæsenet.

Du er personlig ansvarlig for de handlinger, du foretager dig vedr. it og persondata. Det gælder fra du logger på de it-platforme som Køge Kommune stiller dig til rådighed, og til du logger af igen.

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[1]. Så er data beskyttet, sikret backup og kan dokumenteres.

[1] Et fagsystem er fx Aula og eDoc

- 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).

HUSK

- 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.

Proceduren for hhv. datahændelse og sikkerhedsbrud:

- En **hændelse** er en handling, der kan medføre et brud, hvis der ikke reageres rettidigt.
- Et **brud** er, når data ved en fejl eller ulovligt slettes, går tabt, ændres eller offentliggøres.

Eksempler på sikkerhedshændelser kan være:

- Sikkerhedsregler og -procedurer der ikke overholdes
- Phishing mails (forsøg på at franarre en brugers personlige oplysninger)
- Tab af mobiltelefon eller computer, der begge er krypterede

Eksempler på sikkerhedsbrud kan være:

- En e-mail eller besked i Aula, der sendes til den forkerte modtager
- Fortrolige papirer, der ligger tilgængeligt for uvedkommende
- Computere, iPads og telefoner, der ikke låses, når brugeren forlader området/afdelingen
- Personoplysninger på print, der smides i skraldespanden
- Brud på tavshedspligten
- Dokumenter med personfølsomme data, der er journaliseret forkert i e-doc
- Tab af mobiltelefon og computer, der ikke er krypterede
- Taske med fortrolige dokumenter, der glemmes i toget

- Dokumenter med personoplysninger, der ikke håndteres efter forskrifterne, fx dokumenter der ikke bliver låst inde ved arbejdstids ophør

Datahændelse eller sikkerhedsbrud: Hvad gør du?

Kontakt straks nærmeste leder, hvis du oplever et sikkerhedsbrud eller -hændelse.

Hvis du får kendskab til overtrædelser af retningslinjerne, opdager forsøg på uautoriseret adgang til kommunens systemer eller andre uregelmæssigheder, skal du hurtigst muligt informere nærmeste leder. Hvis dette – i en hastesag – ikke er muligt, skal man henvende sig direkte til Informationssikkerhed@koege.dk eller kontakte IT's ServiceDesk på mail 2082@koege.dk eller tlf. 56 67 20 82.

Du kan læse mere om gode råd, tips og tricks og se videoer om sikkerhedsbrud og datahændelse på Dokken.

Hvis du overtræder retningslinjerne, f.eks. ved at misbruge personfølsomme oplysninger eller ved at miste eller lække oplysninger, kan det have store konsekvenser for Køge Kommune f.eks. negativ presseomtale, tab af omdømme og i sidste ende kan det medføre politianmeldelse og store bøder til Køge Kommune.

Beredskabsplan ved sikkerhedsbrud

Skolerne skal bruge deres lokale beredskabsplan ved databrud (hvis beredskabsplan ikke er lavet, skal den udfærdiges snarest).

Beredskabsplanen skal være opdateret og udarbejdes efter retningslinjer fra BUF.

Adgang til systemerne og god IT-kodeks

Som ansat i Køge Kommune folkeskoler, har du adgang til platformene Aula, MinUddannelse, Office365 samt andre digitale platforme. En del af disse platforme indeholder en række personoplysninger, som også kan være følsomme eller fortrolige. Adgangen sker med dit UNI-login, som er personligt. Det er vigtigt, at du **aldrig** giver din kode til andre.

Du må kun benytte systemerne, hvis det er i forbindelse med dine egne arbejdsopgaver. Du må fx **ikke** søge på tilfældige borgeres, families, dine venners eller nabos oplysninger. Derudover må du ikke foretage usaglige opslag, herunder

private opslag i kommunens systemer.

Når du forlader din computer, skal du aktivere din pauseskærm med adgangskode. Du låser din computer ved at trykke samtidig på tasterne:

Kommunikation imellem medarbejdere, elever og forældre

Al kommunikation med personoplysninger med forældre/elever skal ske via Aula. Øvrig kommunikation foregår i Aula eller med din mailadresse, der ender på @koegeskoler.dk. Det er IKKE tilladt at anvende private e-mailadresser, såsom Google, Hotmail, etc. Brug af private e-mails i en arbejdsrelateret sammenhæng kan anses som databrud.
Personfølsomme oplysninger kan du sende og modtage i Aulas beskedsystem opmærket som "følsomt".
Forskellen på personoplysning og følsomme personoplysninger er beskrevet i senere afsnit.

Medarbejdere må ikke være venner med, følge eller på anden måde have private forbindelser til elever på sociale medier. Kommunikation mellem medarbejdere og elever skal altid foregå via de godkendte kommunikationskanaler, herunder Aula. Det er ikke tilladt at dele, sende eller modtage private billeder, videoer eller andet privat indhold med elever via sociale medier eller private digitale platforme. Denne adskillelse mellem den professionelle og private relation skal medvirke til at beskytte både elever og medarbejdere.

Sikkerhed mod virus mv.

Besvar ikke uønskede reklame-e-mails (spam). Alle e-mails scannes automatisk for virus, men vær alligevel opmærksom hvis en e-mail er fra en afsender, du ikke typisk modtager e-mails fra. Er du i tvivl, så kontakt din lokale IT-vejleder eller din nærmeste leder.

Personoplysninger

Informationssikkerhed handler om, at vi skal beskytte enhver form for information, der kan bruges til at identificere en person, og omfatter elektroniske såvel som ikke elektroniske oplysninger.

Personoplysningerne skal opbevares på en sådan måde, der sikrer, at uvedkommende ikke kan få adgang til dem. Nedenfor kan du se, hvornår du skal være særlig påpasselig:

Begreber	**Kategorier**	**Systemer**
Almindelige personoplysninger	Kontaktoplysninger: - Telefonnummer - E-mail - Adresse Identifikationsoplysninger: - Navn - Fødselsdato - Billede - IP-adresse (i hjemmet) - Sygedage I forhold til forældrene: - Familieforhold - Bolig/Bil mm. - Stilling/Job/CV	Skal anvendes respektfuldt. Må ligge i Teams / OneDrive, så længe der er et formål, og det er et arbejdsdokument.
Fortrolige personoplysninger	- CPR nr. - Sociale problemer	Må maksimalt ligge 30 dage i Teams / OneDrive. Upload til Aula. ➔ Brug Aula eller E-doc

		Er du færdig med dokumentet, før de 30 dage følges samme procedure. I Aula markeres oplysningen som følsom.
Følsomme personoplysninger	- Race og etnisk oprindelse - Politisk overbevisning - Religiøs eller filosofisk overbevisning - Genetiske data - Biometriske data med henblik på entydig identifikation (fx fingeraftryk) - Helbredsoplysninger - Seksuelle forhold eller seksuel orientering	Må kun anvendes, hvis der er lovhjemmel til det og så længe oplysningerne er nødvendige. Må maksimalt ligge 30 dage i Teams / OneDrive. Upload til Aula. ➔ Brug Aula eller E-doc Er du færdig med dokumentet, før de 30 dage følges samme procedure. I Aula markeres oplysningen som følsom.

Opbevaring af dokumenter med personligt indhold

Personfølsomme oplysninger om barnet skal gemmes og opbevares i Aula mappe "Sikre filer". Upload filer fra dit OneDrive til Aula.

E-doc kan også bruges til opbevaring af filer af personfølsomkarakter.

Personfølsomme oplysninger om personale skal opbevares i personalemappen i Opus. Se oversigt sidst i denne folder.
Gemmer du et dokument med personoplysninger på din computer, f.eks. i M365, må det max opbevares i 30 dage eller så længe du arbejder på sagen. Derefter skal filen uploades fra dit OneDrive til Aula og du skal slette filen i M365.

Du skal også være opmærksom på, at når du downloader en fil med personfølsomme oplysninger, så gemmes en kopi i mappen "Overførsler". Den fil skal også slettes. Du finder mappen i stifinder (illustration 1).

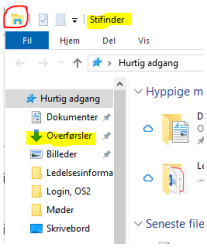

Illustration 1

Husk ligeledes at slette dine slettede filer i "Papirkurv", som du finder på Skrivebordet (illustration 2).

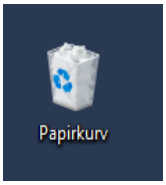

Illustration 2

Du har selv ansvar for at åbne, tømme og behandle e-mails i din personlige postkasse.

Print og personfølsomme oplysninger

Vær opmærksom på adgangsforholdene til de fælles printere, når du printer materiale med personoplysninger. Hent dit materiale straks, så det ikke ligger frit tilgængeligt. Når du er færdig med at bruge materialer med personoplysninger, skal du makulere det. Bemærk også, at materiale med personoplysninger ikke må ligge frit uden opsyn. Det er dit eget ansvar, at materialet bliver låst forsvarligt inde eller makuleret.

Billeder (foto og video)

Fra august 2022 skete der en ændring i brugen af samtykker i Aula.
Der bliver ikke længere skelnet mellem portræt- og situationsbilleder, og visningen af billeder i Aula er ikke længere afhængig af, om der er givet samtykke.

Forældre skal stadig angive, om de giver samtykke til at deres kontaktoplysninger må gemmes og deles. Derimod vil de ikke længere skulle give samtykke til, at fotos og andre medier bliver gemt og delt i Aula. Det gælder både portrætfotos, billeder i galleriet samt videoer og lydfiler.

Medarbejdere

I forhold til foto og video af medarbejderne så afklares tilladelser og rettigheder lokalt.

Fysiske ophæng af fotos på skolen

I må gerne have fysiske billeder af eleverne hængende i klasserne, men minimer brugen af fotos og øvrige personoplysninger, der hænger i fællesrummene og på gangene.

I klasserne kan I have billeder hængende med flere informationer om elever, hvis I ønsker dette. Det kan fx være elevens fødselsdag, forældrenes navne m.v.

Klassebilleder

På mange skoler tages der årligt klassebilleder af ekstern fotograf.
Det anbefales, at alle skoler inddrager skolebestyrelsen i beslutningen om hvorvidt, der tages klassebilleder til fx ophæng på skolernes gange eller til salg til elever og forældre. Dette kan for eksempel ske ved en årlig drøftelse med skolebestyrelsen, så der er en accept og synlighed om skolens tilgang til klassebilleder.
Skolen må gerne have et klassebillede hængende i klasselokalet eller på gangen.

Særligt for forældre

Ved særlige begivenheder som Lucia-optog mv. kan der komme tvivl om, hvorvidt forældre må tage billeder.
Datatilsynet skriver, at hvis man kun tager billeder til egen brug, er det en rent privat aktivitet og dermed slet ikke omfattet af GDPR. Forældrene må derfor tage billeder til egen brug.
OBS: Hvis forældre har lyst til at dele billederne med en større kreds - fx ved at offentliggøre dem på nettet - gælder de databeskyttelsesretlige regler. Børn har ifølge General Data Protection Regulation (GDPR) krav på en særlig beskyttelse. Hvis en

forælder lægger et billede op på sin egen profil på et socialt medie af en situation fra skolen, er det forældrene, der er ansvarlig for behandlingen af personoplysninger.

Skolens myndighedsudøvelse

Skolen har lovhjemmel til at være myndighedsudøvende. Det betyder, at skolen, som en del af det offentliges virksomhed, kan træffe beslutninger om fremvisning af produkter fremstillet i undervisningssammenhæng. At have myndighed og at kunne udøve myndighed, er at have lovlig magt til på skolen at kunne træffe beslutninger – også når det vedrører udstillinger, billeder og elevprodukter.
Som eksempler:

- I forbindelse med et undervisningsforløb i dansk, indskolingen må skolen gerne udstille og dermed udskifte elevfiguren Vitellos hoved med et billede af hver enkelt elevs.
- I historie eller samfundsfag må elevproducerede plancher, der fx angiver politiske udsagn, brug af kildehenvisninger og analyser gerne hænge som udstilling på skolens gange.
- Udstilling af eksamensprojekter fx i forbindelse med valgfaget billedkunst, må ligeledes gerne udstilles på skolen, fx i pædagogisk læringscenter (PLC) eller i kantinen.

Internet

Som medarbejder kan man frit anvende internettet til arbejdsmæssige formål. Endvidere har man mulighed for at anvende internettet til private formål uden for arbejdstiden og i pauser.

Når du er på internettet, afsætter det digitale spor, som kan spores tilbage til Køge Kommune. Du skal derfor altid opfatte dig selv som ambassadør for kommunen og kun anvende internettet i kommunes interesse. Vi ønsker ikke at blive identificeret med private diskussionsfora, porno, racisme og lignende.

Hvis du er i tvivl eller har spørgsmål, så kontakt din nærmeste leder.