KAEF
karise efterskole

Sikker behandling af personoplysninger og informationsaktiver

Kære kollega

Som medarbejdere på Karise Efterskole bærer vi et fælles ansvar for, at informationer bliver håndteret på sikker vis. Hvad enten det er data i vores systemer, dokumenter på vores skriveborde eller den viden, vi har opbygget gennem vores arbejde, så skal vi være opmærksomme på, om disse informationer må deles med andre – både i og udenfor organisationen.

Vi har ikke kun fokus på informationssikkerheden på efterskolen, fordi lovgivningen pålægger os at løfte det ansvar. Vi ønsker også som organisation, at vores brugere og medarbejdere skal have tillid til, at vi i organisationen forvalter den viden og de relationer, vi opbygger på forsvarlig vis.

Informationssikkerhed bliver derfor et kerneelement i tillidsforholdet mellem organisationen og vores brugere og samarbejdspartnere.

Ved at læse og følge retningslinjerne i denne pjece medvirker vi alle til at opretholde og styrke tillidsforholdet mellem efterskolen og vores samarbejdspartnere. I praksis drejer det sig om at udvise omtanke og handle derefter, når vi har med data, dokumenter og viden at gøre.

Du skal huske

Retningslinjerne for it-adfærd i denne pjece skal følges af samtlige medarbejdere på Karise Efterskole

Etisk it-adfærd

Når vi som medarbejdere repræsenterer efterskolen, er det vigtigt, at vi udviser sund fornuft. Det gælder både vores daglige brug af it-systemer og vores forvaltning af personoplysninger.

Vi skal ikke blot overveje, om vores adfærd er forsvarlig i forhold til lovgivningen og vores egne politikker, men også bruge vores dømmekraft i forhold til etiske spørgsmål. Eksempelvis når vi deltager i debatter på sociale medier.

Du skal huske

… at bruge din sunde fornuft, når du som medarbejder er på sociale medier, eller når du tilgår eller deler informationer som en del af dit arbejde.

… at det kan være ulovligt og strafbart at opbevare eller dele copyright-beskyttede filer, som for eksempel musik eller film, med dine kolleger.

… at fortrolige informationer ikke bare er dokumenter eller data. Det kan også være den viden, du har tilegnet dig gennem dit arbejde. Sammenfattende kalder vi disse for informationsaktiver, uanset om de er elektroniske, i papirform eller videregivet i samtale.

Dine brugeroplysninger

Vi betragter brugernavne, og især de adgangskoder, der hører til, som strengt fortrolig information. Du må derfor ikke dele din adgangskode med andre – hverken i eller udenfor organisationen.

I de fleste tilfælde har vi sat regler op, der automatisk sætter grænser for hvor simple adgangskoder, du kan oprette i it-systemerne. Men du kan sikre dig yderligere mod misbrug ved at vælge en adgangskode, der ikke er let at gætte.

Vælg derfor altid en adgangskode, der er let at huske for dig, men som ikke giver mening for andre. Du kan for eksempel vælge en huskesætning som:

Min **s**østers **h**und **F**ido **h**ar **3 b**en**!**
= MshFh3b!

Du skal huske

… at ændre din adgangskode med det samme, hvis du har mistanke om, at andre kender den.

… at du ikke må skrive din adgangskode ned – hverken på papir eller i ikke-krypterede filer, som andre kan få adgang til.

... at du ikke må oplyse din adgangskode til andre – hverken via telefonen eller personligt.

Klassifikation af informationer

For at vi som medarbejdere har de bedst mulige betingelser for at beskytte vores informationsaktiver korrekt, inddeles de i tre overordnede kategorier:

Offentlig
Ikke-fortrolige informationsaktiver, som frit kan benyttes af alle. Det gælder for eksempel alt indhold på internettet, der kan tilgås uden login.

Intern
Alle interne informationsaktiver, der kun er tiltænkt medarbejdere, samarbejdspartnere og leverandører.

Fortrolig
De informationsaktiver, som typisk kun må tilgås af få godkendte brugere, som for eksempel personoplysninger. De må kun deles med eksterne, hvis begge parter har underskrevet en databehandleraftale - Disse aftaler står ledelsen for.

Du skal huske

… at alle informationsaktiver, der er klassificeret som **intern** eller **fortrolig**, skal opbevares i aflåste områder (eller it-systemer med individuel adgangskontrol), når de ikke anvendes.

… at gæster ikke må efterlades uden opsyn i områder med **fortrolig** information.

… at informationsaktiver, der endnu ikke er blevet klassificeret, som udgangspunkt er klassificeret som **intern**.

... at viske eventuelle whiteboardtavler rene og fjerne diverse papirer, når du forlader dit skrivebord eller et mødelokale.

Opbevaring af informationer

For at beskytte efterskolen mod tab af data skal du så vidt muligt undgå at gemme filer på lokale drev, usb-nøgler eller andre lokale lagermedier. Ved at gemme dine filer på filserveren/365/One Drive eller i vores administrative SharePoint it-systemer vil der blive taget backup af dine filer.

Du skal huske

HUSK BACKUP

Arbejde på kontor

Du er ansvarlig for de informationsaktiver, du omgås i dit arbejde. Det inkluderer dokumenter, data, services, systemer, software, hardware og viden. Det er essentielt, at du arbejder med opmærksomhed og forsigtighed for at beskytte efterskolens informationer.

Cleandesk
Efterskolen har en cleandesk politik. Det skal blandt andet være med til at mindske risikoen for, at følsomme oplysninger mistes.
Cleandesk politikken betyder, at du skal rydde alle papirer, dvd'er, usb-nøgler og andre medier væk, når du forlader dit skrivebord, som kan indeholde personfølsomme data.

Lås computeren
Når du forlader dit skrivebord, skal du huske at låse computeren.

Du skal huske

… at alle gæster og besøgende på Karise Efterskole skal modtages af deres vært i receptionen, være under opsyn under deres besøg, og eskorteres til udgangen, når de afslutter besøget.

… at du derfor skal være opmærksom på, om der er gæster eller andre i området, som uforvarende kan få kendskab til interne/fortrolige informationsaktiver.

Tag medansvar for, at det ikke sker!

365 Arbejde – lån af andres udstyr

Hvis du udfører fjernarbejde fra en computer, tablet eller smartphone, der ikke er efterskolens, har vi ikke mulighed for at sikre og kontrollere udstyret. Det er derfor særdeles vigtigt, at du ikke arbejder med informationer klassificeret som fortrolig på it-udstyr, der ikke er efterskolens.

Så vidt muligt skal du undgå at overføre informationer mellem dit private udstyr og fondens udstyr via
e-mail, usb-nøgle, cloud services mv., da det øger risikoen for softwareangreb og datalækager.

Du skal huske

… at du ikke må dele din bærbare arbejdscomputer med ægtefælle, børn, venner og andre, hvis du tager den med hjem. Det er for at mindske risikoen for uagtsomt at videregive følsomme informationer.

Mobile enheder og print

Mobile enheder som smartphones og bærbare computere kan indeholde store mængder informationer. Derfor forsøger vi at holde et højt sikkerhedsniveau fra centralt hold, for eksempel i form af kodeord, pinkode, fingeraftryk, datakryptering, fjernsletning af enheder mv.
Der må kun bruges native apps, programmer som outlook eller programmer som er godkendt af efterskolen.

Du må under ingen omstændigheder forsøge at slå disse sikkerhedsfunktioner fra, da de er indført for at sikre vores informationsaktiver.

Print
For at reducere miljøbelastning og risiko for datalækager er det vigtigt, at du udskriver så lidt som muligt. Overvej altid, om informationerne kan videregives digitalt.

Du skal huske

… at personoplysninger også skal beskyttes i fysisk form. Udskrifter, der indeholder personoplysninger, må derfor ikke efterlades uden opsyn, med mindre de opbevares aflåst.

Hardware og software

På efterskolen gør vi hvad vi kan for at sikre det it-udstyr, vi alle benytter i vores daglige arbejde er sikret og up to date. Desværre er det ikke muligt at sikre mod alt, og det er derfor vigtigt, at du hjælper med at mindske risikoen for it-angreb.

Eksempelvis er der en høj risiko for overførsel af skadelig software, hvis du tilslutter en usb-nøgle til en ekstern computer og så bagefter til en arbejdscomputer.

Du må derfor aldrig tilslutte fremmede/gæster enheder til vores interne Kaudd - laerernetværk, gæster skal tilgå Kaudd Guestnet.

Du skal huske

… at niveauet af sikkerhed på vores it-udstyr i høj grad afhænger af, at du anvender det med omtanke og ikke bevidst forsøger at omgå sikkerhedsindstillingerne.

… at der ikke findes noget, der er 100% sikkert. Der kommer løbende nye angrebsformer, der kan omgå sikkerhedssystemer, men næsten alle angreb skal aktiveres af brugeren. Du spiller altså en væsentligt rolle i at sikre vores informationsaktiver.

… at brug af piratkopieret software naturligvis ikke er tilladt
... Altid opdatere når systemet beder dig om det

Brug af e - mail

Vores e-mailsystemer er beskyttet bedst muligt, men det er desværre umuligt at blokere for al ondsindet software. Det er derfor vigtigt, at du er ekstra forsigtig, inden du åbner vedhæftede filer eller trykker på weblinks i e-mails. Er du i tvivl, så spørg hellere en gang for meget end en gang for lidt.

Din e-mail til arbejdet er kun beregnet til arbejdsrelateret brug. Den må kun benyttes privat i begrænset omfang. Ønsker du at beskytte private
e-mails, skal du placere dem i en undermappe, som du navngiver "Privat". Så kan vores it-ansvarlige se, at det er private e-mails, som ikke umiddelbart må læses af andre (for eksempel i forbindelse med ferie eller sygdom).

Du skal huske

… at personoplysninger **kun** må deles med tredjeparter, der har underskrevet en databehandleraftale. Det er for at leve op til lovgivningskrav om, at kunne dokumentere, at kun godkendte tredjeparter har adgang til de personoplysninger, vi behandler.

… at private e-mails i sagens natur er private. Derfor anbefaler vi, at du bruger en anden løsning end din arbejdsmail til private korrespondancer.

… hvis du er i tvivl/usikker kontakt kontoret, og forhør dig om der er lavet af databehandleraftaler.

Brug af internet

Når du anvender efterskolens udstyr til at gå på internettet, repræsenterer du efterskolen.

Internetadgangen er tiltænkt at være et værktøj, der benyttes til at udføre arbejdsrelaterede opgaver. Personlig brug i begrænset omfang er tilladt, men det må ikke forstyrre dit eller andres arbejde. Brug af internettet skal være etisk forsvarlig og må ikke bryde dansk eller europæisk lovgivning.

Virus og malware
Vores sikkerhedssystemer blokerer for så mange websites, der indeholder kendt skadelig software eller bryder etiske regler og dansk lovgivning, som muligt.
Desværre er filtreringen ikke perfekt, så det er vigtigt, at du altid udviser omhu og tænker dig om, når du anvender internettet, specielt når du er på hjemmenetværk eller ude byen med dit udstyr.

Du skal huske

… at undlade at besøge websider, du ikke føler dig tryg ved.

… at være opmærksom på, at mange websider kun eksisterer med det formål at lokke informationer ud af de besøgende. Kig efter stavefejl og vær særligt opmærksom i forbindelse med netbank eller andre sider, der benytter Nem ID.

… at dit udstyr kan spores tilbage til vores offentlige IP-adresse på internettet, når du går på nettet via Efterskolens internetforbindelse.

Brug af Sociale medier

Du er ansvarlig for de informationer, du offentliggør på internettet, uanset om det er på et nyhedsmedie, en blog, Facebook, LinkedIn, Twitter eller andre medier.
Vær derfor opmærksom, inden du offentliggør noget - det kommer sandsynligvis til at være tilgængeligt på internettet i lang tid og kan være meget vanskeligt at fjerne igen.

Brug af sociale medier må absolut ikke benyttes til at dele informationer klassificeret som intern eller fortrolig. Vi bruger sociale medier meget i vores organisation, og det er derfor vigtigt at holde tungen lige i munden når vi deler. Vær opmærksom på hvilken profil/side du deler fra og hvad du deler. Har du hjelm til at dele de fotos? Samtykkeerklæringer

På sociale medier er det desuden vigtigt, at du tydeligt gør opmærksom på, at holdningerne, du deler, er dine egne og ikke efterskolens.

Der skal ligeledes indhentes Samtykkeerklæringer fra de studerende, hvis de figurerer på efterskolens FB sider.

Du skal huske

… at udtalelser på efterskolens vegne bør koordineres med den kommunikationsansvarlige eller direktionen.

... at respektere persondataloven, ophavsret, og hvordan du offentliggør informationer, du ikke selv har skrevet – inden du gør det.

… at være opmærksom på de oplysninger, du deler på sociale medier – de kan misbruges af hackere.
… indhente samtykkeerklæringer fra de studerende, hvis der bruges foto.

Alarmering

Sikkerhedshændelser indtræffer. Hvad enten det er virusangreb, at informationsaktiver er faldet i de forkerte hænder, eller at en tredjepart har fået uautoriseret adgang, så skal du altid henvende dig samme sted:

Kontoret
Rønne Alle 7
4653 Karise
56767400

Ring på telefon hvis uheldet er ude.
91895406
Samir Christian Hyge Sabri
DPO – ansvarlig
Karise Efterskole

Du skal huske

… at henvende dig til vores it-ansvarlige øjeblikkeligt, hvis du har mistanke om, at din computer eller smartphone er inficeret med ondsindet software. Så kan en specialist nemlig undersøge omfanget af skaden, herunder hvor meget softwaren har spredt sig til andre systemer.

... at være på vagt og bruge din sunde fornuft – uanset om du arbejder på kontoret eller hjemmefra.

Sikkert digitalt arbejde

Yderligere oplysninger om informationssikkerhed vil blive udarbejdet og introduceret løbende, ligesom der vil blive afholdt informationsmøder med opdateringer om emnet.

Skulle du have en god ide til at styrke efterskolens informationssikkerhed, hører vi meget gerne fra dig!

Venlig hilsen
Samir Christian Hyge Sabri

Dette dokument er klassificeret: Offentligt

GDPR

Internt i virksomheden

- Fortegnelsen
- Persondatapolitikker (intern)
- Risikovurderinger
- Procesbeskrivelser for sletning og databrud
- Medarbejderinstrukser

Tredjeparter

- Databehandleraftaler
- Underdatabehandleraftaler
- Fælles dataansvarlige aftaler
- Overførselsgrundlag ved overførsel til tredjelande
- Hemmeligholdelsesaftaler (NDA)

De registrerede

- Persondatapolitik (ekstern)
- Proces for overholdelse af de registreredes rettigheder
- Dokumentation af korrekt svar til registrerrede
- Samtykkeerklæringer

Løbende kontrol

- Egenkontrol
- Kontrol med databehandlere
- Systemkontrol
- DPO kontrol
- Registrering af hændelser
- Konsekvensanalyser (DPIA)