Designskolen Kolding

Informationssikkerhedspolitikker

ISO27001:2013, ISO27001:2023 & ISO 27002:2022

Melanie Truhr

23-04-2025

Versionshistorik

- Opdateret på baggrund af Persondataforordningen (GDPR) d. 25.5.2018.
- Revideret d. 19-06-2020
- Revideret d. 12-01-2022
- Revideret d. 01-11-2023
- Revideret d. 24-10-2024 (tilføjet nye ISO)
- Revideret d. 16-01-2025 (formel redigering)
- Godkendt af Rektoratet d. 17-03-2025

Informationssikkerhedskoordinator

- Trine Lumbye - Chef for administration og forretningsudvikling, prorektor
- Melanie Truhr – IT-specialist

Informationssikkerhedsudvalget

- Trine Lumbye - Administrationschef, prorektor
- Melanie Truhr – IT-specialist
- Henrik Nyhuus Gill – System-administrator
- Lene Nyhus Friis - Projektchef og leder af Lab for Leg og Design, Lab for Socialt Design og Lab for Bæredygtighed og Design
- Pernille Thøstesen – økonomichef
- Jette Ladegaard Garnæs – studiechef
- Eva Kappel – Chef for uddannelse
- Christina Stind Rosendahl - Kvalitetskoordinator, forsknings- og udviklingssekretær
- Anette Flinck – Ansvarlig for internationale relationer

DPO

Melanie Truhr – IT-specialist

Lov og krav

- ISO27001:2013
- ISO27002:2022
- ISO27001:2023

Indholdsfortegnelse

Indledning

Designskolen Kolding (DSKD) følger de anviste lov og krav der er i hht. databeskyttelsesforordningen også kaldt GDPR. Dette er for at skabe trygge rammer for medarbejdere, studerende og andre involverede interessenter. DSKD har mange funktioner som administration, undervisning og forskning, hvilket berører data- og personfølsomme data. DSKD har derfor vedtaget rammer for, hvordan man håndterer disse forskellige typer af data.

5 Formål med informationssikkerhedspolitikken

DSKD informationssikkerhedspolitik er vores sikkerhedsgrundlag og vores fælles forståelse af, hvad informationssikkerhed er.

Informationssikkerhedsstrategien og informationssikkerhedspolitikken fastlægger vores ambitionsniveau og opstiller rammerne for de sikkerhedstiltag, som er nødvendige at følge, når vi som en organisation med samfundsmæssig betydning skal leve op til lovgivningskrav og "Best practices".

DSKD ser ikke kun et højt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetselement i forhold til at kunne tilbyde en sikker service over for samarbejdspartnere, myndigheder, medarbejder og primært vores studerende.

Med informationssikkerhed forstår vi den nødvendige beskyttelse af samtlige ressourcer, der indgår i eller bidrager til DSKD's behandling og kommunikation af data, der kan forekomme både elektronisk, i papirform samt tale. Herunder også i teknologi og organisatoriske processer.

5.1. Retningslinjer for styring af informationssikkerhed

5.1.1 Politikker for informationssikkerhed

DSKD´s informationssikkerhedspolitik skal offentliggøres og kommunikeres til alle relevante interessenter, herunder især medarbejdere, studerende og samarbejdspartnere.

Informationssikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet i overensstemmelse med gældende persondataforordning (GDPR). Foranstaltninger inkluderer tekniske, proceduremæssige, lov- og regelmæssige kontroller.

Informationssikkerhedspolitikken skal godkendes af rektoratet (ISO27001:2013).

5.1.2 Gennemgang af politikker for informationssikkerhed

Politikkerne for informationssikkerhed skal årligt gennemgås af informationssikkerhedsgruppen for at sikre deres fortsatte egnethed, tilstrækkelighed og aktualitet samt væsentlige lovændringer/krav er overholdt (ISO27001:2013).

5.1.3 Dokumenteret drift procedurer hos DSKD

Driftsprocedurer for informationsbehandlingsfaciliteter bliver hos DSKD dokumenteret og gøres tilgængelige for de medarbejdere, der har brug for dem. Dette har til formål at sikre korrekt og sikker drift af informationsbehandlingsfaciliteter, samt sikre at medarbejdere hos DSKD ikke er i tvivl om, hvordan de håndterer det givende IT-system/systemer de sidder med i den daglige drift (ISO27002:2022, 5.37).

6 Organisering af informationssikkerhed

IT- og Informationssikkerheden på DSKD er styret af klare retningslinjer og regler samt en tydelig ansvarsfordeling. Ansvaret er hierarkisk placeret med skolens øverste ledelse, rektoratet, som hovedansvarlig for overholdelse og implementering af informationssikkerhedspolitikken, både internt og i samarbejdet med eksterne partnere.

6.1 Interne organisatoriske forhold

Rektoratet har det øverste ansvar for informationspolitikken og har i denne kapacitet valgt at uddelegere dele af ansvaret til relevante funktioner og udvalg.

6.1.1 Roller og ansvarsområder for informationssikkerhed

Administrationschef og prorektor Trine Lumbye har som informationssikkerhedskoordinator det overordnede ansvar for informationssikkerhed og rapporterer direkte til ledelsen som herefter informerer rektor.

IT-specialisten fra IT-afdelingen skal som databeskyttelsesrådgiver (DPO) inddrages i alle spørgsmål om databeskyttelse og har en rådgivende og overvågende funktion om de databeskyttelsesretslige regler, især med fokus på behandlingen af personfølsomme oplysninger herunder især på områder, hvor der er større risiko for uretmæssigheder. DPO´en er også kontaktperson for og til Datatilsynet. Derudover har DSKD et antal dataejere, som er registreret i et dataejerdokument (Bilag 1, Rollekatalog, 2024), som er et internt bilag til DSKD´s Informationssikkerhedspolitik.

Ansvaret for den daglige drift ligger hos systemejer og systemansvarlig, og sikkerhed er placeret hos systemadministratorerne, der rapporterer til informationssikkerhedskoordinatoren. DSKD´s samarbejdsudvalg er samtidig skolens informationssikkerhedsudvalg og har ansvar for at sikre, at politikken for informationssikkerhed er synlig, koordineret og i overensstemmelse med DSKD´s strategi (ISO27001:2013).

6.1.2 Ledelsens ansvar

Ledelsen hos DSKD tilkendegiver sin støtte til DSKD´s informationssikkerhedspolitik, emnespecifikke politikker, procedurer og informationssikkerhedsforanstaltninger. Der er ledelsen og IT-specialisten som sikrer at alle interessenter er orienteret, og at DSKD har kompetente medarbejdere til at håndtere DSKD´s informationssikkerhed samt hertil hørende lov og krav (ISO27001:2022, 5 og ISO27002:2023, 5.4).

6.1.3 Funktionsadskillelse

Systemadministratorerne er ansvarlige for den daglige drift, som nævnt i tidligere afsnit (jf. 6.1.1)

6.1.4 Kontakt med myndigheder

Informationssikkerhedskoordinatoren er i samspil med DPO´en ansvarlig for anmeldelser til Datatilsynet, herunder for eventuelle brud på Persondataforordningen indenfor 72 timer efter et sådant

brud opdages. Anden myndighedskontakt foretages af Informationssikkerhedsudvalget, når det vurderes relevant. (ISO27001:2013).

6.1.5 Kontakt med særlige interessegrupper

IT-afdelingen skal gennem abonnement på relevante nyhedsbreve og sikre sig i samarbejde med relevante leverandører adgang til opdateret viden om sikkerhed, risici, beskyttelsesmetoder og -værktøjer. Relevante interessenter skal informeres om informationssikkerhedspolitikken på DSKD. Samtidig deltager en repræsentant for IT-sikkerhedsudvalget i DeiC's DPO-netværk og DSKD følger DS (DanskStandard) standarder for at sikre, at lov og krav er opfyldt (ISO27001:2013, ISO27001:2022 og ISO27002:2023).

6.1.6 Informationssikkerhed ved projektstyring

I forbindelse med alle projekter, både interne og eksterne, skal organisationens regler og gældende lovgivning for beskyttelse af materiel samt data overholdes af alle involverede i projektet/projekterne (ISO27001:2013, ISO27001:2022).

6.1.7 Informationssikkerhed ved brug af cloudtjenester

DSKD har fastlagt processer for anskaffelsen, brug, styring og afslutning af brugen af cloudtjenester i overensstemmelsen med DSKD´s informationssikkerhedskrav. Dette er for, at DSKD kan styre informationssikkerheden i hht. brugen af cloudtjenester (ISO27002:2022, 5.23).

6.3 Mobilt udstyr og hjemmearbejde

Skolens medarbejdere benytter sig i vid udstrækning af mobilt udstyr/enheder, og informationssikkerhedspolitikken indeholder derfor klare regler for lån/brug af disse (ISO27001:2013).

6.3.1 Mobilt udstyr

Alt mobilt udstyr, herunder computere og telefoner, skal beskyttes med password og/eller biometrisk visning (fx Touch ID, ansigtsgenkendelse). Udleveret udstyr/enheder fra DSKD, er strengt personligt og må kun benyttes af medarbejderen, enheden/enhederne er udleveret til. Medarbejderen hæfter for skader påført udstyret af andre, hvis udstyret har været brugt uden for arbejdsmæssig sammenhæng. De udleverede udstyr/enheder må ikke benyttes som host for servere og bit-torrent-programmer eller til at tilgå andet ulovligt materiale, hvor fx ophavsrettigheder ikke overholdes. Mobiltelefoner benyttes i overensstemmelse med abonnement (Bilag 5, Brug af udlånt mobiltelefon) (ISO27001:2013).

6.3.2 Hjemmearbejde

Det er ikke muligt at få stillet en egentlig fjernarbejdsplads til rådighed, men udleveret mobilt udstyr/enheder må benyttes som sådan via VPN-opkobling ifølge ovenstående politik for mobilt udstyr (jf. afsnit, 2.3.1).

Ved hjemmearbejde eller i det hele taget arbejde udenfor skolen gælder de samme regler for IT-sikkerhed og beskyttelse af data som ved arbejde på skolen, herunder låsning af skærm, når computeren forlades samt beskyttelse af persondata og fortrolige data.

Samtidig må der ikke opbevares persondata og fortroligt data på privat udstyr. (ISO27001:2013).

Når der arbejdes uden for DSKD´s fysiske rammer skal man stadig agere hensigtsmæssigt og følge DSKD´s politikker. Når man ikke er koblet på DSKD´s VPN-opkobling og arbejder uden for DSKD`s netværk, skal man være opmærksom på, hvilket netværk man arbejder på for ikke at risikere cyberkriminalitet.

For at skabe optimal og sikker adgang til IT-systemerne, der anvendes i daglig drift på DSKD, gives der adgangsmulighed til mindst to medarbejder. Dette er for at sikre, at der altid er en medarbejder på DSKD fysisk, som har adgang til det respektive IT-system/systemer (ISO27002:2022, 6.7).

6.3. Anvendelse af software til videokonferencer

På DSKD tilbyder vi forskellige typer af videokonferencesoftware (Bilag 6, Data typer og håndtering heraf)

Fælles for disse er, at man kun må benytte sådan software, hvis man benytter sit DSKD-login. Mødelink er ikke i sig selv personlige eller private, og der skal derfor være ekstra opmærksomhed på, hvordan disse beskyttes i forbindelse med fortrolige møder, da alle i organisationen har adgang til alle møder med offentligt delte mødelink (Bilag 4, Retningslinjer for video møder).

Der gøres opmærksom på, at man ikke må dele optagelser eller billeder fra mødet uden alle mødedeltageres accept (ISO27002:2022).

6.4. Samarbejder med eksterne

I samarbejde med eksterne, hvor der behandles persondata, skal der forelægge en databehandleraftale.

I de samarbejder, hvor DSKD´s data bliver behandlet af eksterne parter, er DSKD ansvarlig for at indgå en databehandleraftale med den eksterne databehandler.

DSKD har med udgangspunkt i Datastyrelsens databehandleraftale udarbejdet en skabelon for databehandleraftaler, som den dataansvarlige medarbejder skal udfylde i forbindelse med indgåelse af samarbejde med eksterne databehandlere.

I de samarbejder, hvor DSKD´s medarbejdere indgår i samarbejder med eksterne om disses data, er DSKD at betragte som databehandler, og det er således den eksterne parts ansvar at udarbejde en databehandleraftale.

Det forventes af skolens medarbejdere, at de i en enhver sammenhæng husker på den awareness-træning, de har gennemgået på DSKD samt stiller sig kritisk overfor brugen af persondata og er opmærksomme på beskyttelsen af disse (ISO27002:2022).

6.5 Optagelse og deling af video/billede materiale

Når der optages video eller tages et billede, er det vigtigt at være opmærksom på, at alle der optræder i videoen eller på billedet har givet samtykke. Det er også vigtigt at informere hvor video og billeder bliver delt så de deltagende i videoen eller på billedet/billederne er gjort opmærksom på dette. Ifølge databeskyttelsesforordningen er et samtykke efter udtryk for, at de registrerede – dvs. borgerne, kunderne, medlemmerne el.lign. – gives et reelt valg og kontrol over, hvordan deres oplysninger bruges, og er efter forordningen et af flere – ligestillede – behandlingsgrundlag, som den dataansvarlige kan anvende ved behandling af personoplysninger. (Databeskyttelsesforordningens artikel 4, nr. 11, 2023 - GDPR).

7 Personalesikkerhed

DSKD er opmærksom på at gennemføre en kvalitetsmæssig ordentlig og sikker rekruttering og ”Onboarding”, herunder at nyansatte medarbejdere kvalificeres til at kunne benytte skolens informationsressourcer inden for de i informationssikkerhedspolitikken angivne principper og regler (ISO27001:2013).

7.1 Før ansættelsen

3.1.1 Screening

Alle ansættelsesudvalg vurderer i forbindelse med ansættelsesforløb, om der skal rekvireres personlige referencer samt straffeattest (ISO27001:2013).

7.1.2 Ansættelsesvilkår og -betingelser

Som en del af ansættelseskontrakten giver medarbejderen tilsagn til, at vedkommendes data må opbevares og behandles efter gældende lovgivning. Yderligere accepteres den for skolen til enhver tid gældende IT- og informationssikkerhedspolitik, der beskriver DSKD´s medarbejderes ansvar og forpligtelser vedrørende IT- og informationssikkerhed samt regler for brug af det af skolen udleverede udstyr/enheder (ISO27001:2013).

Det er den ansættende leders ansvar, at den nyansatte medarbejder får udleveret relevant udstyr og introduceres til sikker anvendelse af dette udstyr samt DSKD´s systemer. Samtidig er det den ansættende leders ansvar, at den nye medarbejder informeres om DSKD´s IT- og informationssikkerhedspolitik samt orienteres om, hvorledes data og dokumenter behandles sikkert, samt hvor og hvordan data arkiveres. (ISO27001:2013 og ISO27002:2022).

7.2 Under ansættelsen

7.2.1 Ledelsesansvar

Det er rektoratets ansvar at sikre, at alle medarbejdere er grundigt informeret om kravene til behandling af informationer og brug af udstyr, så alle medarbejdere kan behandle data forsvarligt samt overholde den til enhver tid gældende lovgivning og krav. Det er i samspil med IT-specialisten fra IT-afdelingen at sende disse informationer og materiale ud til de relevante interessenter.

Efter aftale med rektoratet har dataejer i samråd med ansættende leder, ansvaret for tildeling af rettigheder. IT-afdelingen tildeler rettigheden, når IT-afdelingen har fået skriftlig godkendelse af leder. Alle medarbejdere er ansvarlige for at sætte sig ind i og overholde den til enhver tid gældende lovgivning samt Designskolens Koldings regler om IT- og informationssikkerhed. (ISO27001:2013 og 27002:2022, 5.18).

7.2.2 Privatlivsbeskyttelse og beskyttelse af personoplysninger

DSKD identificerer og opfylder kravene vedrørende privatlivsbeskyttelse og beskyttelse af personoplysninger i henhold til gældende love og forskrifter samt kontraktlige krav. DSKD har udviklet og implementeret procedurer for privatlivsbeskyttelse og beskyttelse af personoplysninger. Disse procedurer kommunikeres ud til alle relevante interessenter, der er involveret i behandlingen af personoplysninger 27002:2022 (jf. afsnit 5.34).

7.2.3 Bevidsthed om uddannelse og awareness træning i informationssikkerhed

IT-afdelingen er ansvarlig for løbende at informere både ledelse og medarbejdere om nye tiltag samt nødvendige ændringer i procedurer. Dette er med til at sikre, at alle interessenter på DSKD er opdateret med de nyeste lov og krav.

Alle medarbejdere er ansvarlige for at sætte sig ind i og overholde den til enhver tid gældende lovgivning samt DSKD´s regler om informationssikkerhed (ISO27001:2013).
DSKD gennemfører løbende awareness træning som online kurser, hvor både medarbejder og studerende bliver ført igennem videoer, for at styrke deres viden inden for cybersikkerhed, og hvad man skal være opmærksom på (ISO27002:2022, 6.3).

7.2.4 Kompetencer

DSKD vægter, at medarbejder har hhv. den rette uddannelse, træning eller erfaring for at kunne løfte opgaven de er stillet, og som berør informationssikkerhed. Hvis medarbejderen ikke har kompetencen, fastlægges de nødvendige kompetencer og medarbejderen ajourføres (27001:2023, 7.2).

7.2.5 Sanktioner

Medarbejdere, der bevidst overtræder reglerne for informationssikkerhed, indkaldes til samtale med deres nærmeste leder, der vurderer sagens alvor samt dens eventuelle konsekvenser.

Ved grovere overtrædelser indkaldes til samtale med nærmeste leder samt administrationschefen, der vurderer sagens alvor samt dens eventuelle konsekvenser (ISO27001:2013).

7.2.6 Gennemsigtighed

Medarbejdere giver i forbindelse med tiltrædelsen lov til, at DSKD under ansættelsen opbevarer og behandler deres data og informationer. Disse data og informationer opbevares fortroligt og deles kun med offentlige myndigheder efter aftale med medarbejderen, fx i forbindelse med sygdom. DSKD deler ikke medarbejderdata med tredjepart.

Alle medarbejdere har til enhver tid ret til at få oplyst, hvilke data institutionen ligger inde med om vedkommende. Disse data vil blive gjort tilgængelige for medarbejderen indenfor 14 dage efter aktindsigt (ISO27001:2013).

7.3 Ansættelsesforholdets ophør eller ændring

7.3.1 Ansættelsesforholdets ophør og ændring

Det er nærmeste leders ansvar at orientere IT-afdelingen om fratrædelser og afskedigelser, så IT-afdelingen kan lukke mail-konti, telefonnumre m.v. På sidste arbejdsdag tilbageleverer medarbejderen de udleverede informationsressourcer (computer, mobiltelefon, iPads o.l.).

Når der sker fratrædelse, er det den enkeltes ansvar at sikre de personlige data, der er på det lånte udstyr/enheder, inden udstyr/enheder afleveres. DSKD står ikke til ansvar for disse data og IT-afdelingen og nulstiller udleveret enheder sammen med den tilknyttede bruger af enhederne på afleveringsdagen.

Efter ansættelsens ophør bliver den fratrådte medarbejders AD-konto deaktiveret, herunder mailkonto, der dog henviser til ny medarbejder og/eller nærmeste leder i form af autosvar. Perioden for dette aftales mellem afgående medarbejder og nærmeste leder, dog maksimalt et halvt år.

Ved stillinger i det øverste ledelseslag kan det være nødvendigt at en anden medarbejder får adgang til mailen for at sikre bevarelse af data. Dette aftales også med afgående medarbejder. Samtidig tages der stilling til, om disse mailkonti skal arkiveres på arkivserveren. Sletning af disse aftales med rektor.

Den fratrådte medarbejder har efter ansættelsens ophør ret til at blive glemt, dvs. få alle sine data fjernet fra institutionens arkiver, medmindre dette strider mod anden lovgivning (ISO27002:2022).

Ved barsel returneres de udleverede informationsressourcer medmindre anden aftale indgås med nærmeste leder og den IT-systemansvarlige.

I tilfælde af strejke/lockout i forbindelse med overenskomstforhandlinger skal medarbejdere aflevere det udleverede materiel, medmindre andet besluttes af rektoratet. Efter ansættelsens ophør bliver den fratrådte medarbejders AD-konto deaktiveret, herunder mailkonto, der dog i en måned herefter henviser til ny medarbejder og/eller nærmeste leder i form af autosvar. Det udleverede udstyr/enheder

skal afleveres senest ved fratrædelsesdatoen. Sker dette ikke, kan medarbejderen stille til ansvar for de udgifter DSKD har haft ved det udlånte udstyr/enheder til medarbejderen.

Den fratrådte medarbejder har efter ansættelsens ophør ret til "at blive glemt", dvs. få alle sine data fjernet fra institutionens arkiver, medmindre dette strider mod anden lovgivning. Skulle det være tilfældet bliver den fratrådte gjort opmærksom på dette (ISO27001:2013, ISO27001:2022 og ISO27002:2023).

8. Studerendes rettigheder og sikkerhed

DSKD er opmærksom på at gennemføre en ordentlig og sikker optagelse af nye studerende, så disse introduceres til skolens ressourcer, systemer og regler, herunder for IT- og informationssikkerhed (ISO27001:2013).

8.1. Før optagelse

8.1.1. Ansøgning om studieplads

Så snart en potentiel studerende har ansøgt om optagelse på DSKD, forpligter skolen sig til at behandle persondata i overensstemmelse med Persondataforordningen og anden lovgivning på området.

8.2.1. Optagelse

I forbindelse med ansøgning om optagelse har DSKD hjemmel til at behandle studerendes data efter gældende lovgivning.

Ikke-optagne studerendes data slettes efter endt optagelsesproces.

8.2. Studietid

I forbindelse med brugen af billeder, video, lydoptagelser og tilsvarende medier, der optages på DSKD eller i forbindelse med aktiviteter relateret til DSKD, beder vi de studerende om en samtykkeerklæring. I forbindelse med dette gælder de almindelige regler om samtykke og tilbagetrækning af samtykke (jf. afsnit, 16.3).

8.2.2. Studerendes udstyr og data

DSKD er ikke ansvarlig for indskrevne studerendes udstyr samt indsamling og brug af data.

8.2.3. Bevidsthed om, uddannelse og træning i IT- og informationssikkerhed

DSKD bestræber sig på at informere og uddanne de studerende indenfor IT-sikkerhed og awareness.

IT-sikkerhed er ansvarlig for løbende at informere studerende om pludseligt opstående IT-hændelser samt potentielle risikosituationer.

Alle studerende er ansvarlige for at sætte sig ind i og overholde den til enhver tid gældende lovgivning.

8.2.4. Regler for brug af IT-systemer

DSKD's IT-systemer, servere, netværk m.v. må ikke benyttes til ulovligheder, herunder som host for servere og bit-torrent-programmer.

Virusprogrammer skal installeres og opdateres løbende. Ligeledes skal alle andre programmer og systemer opdateres løbende.

Samtidig skal ophavsrettigheden respekteres, både i forbindelse med billeder, tekst, programmer, video, design etc.

8.2.5. Sanktioner

DSKD kan til enhver tid fjerne den studerendes netadgang/systemadgang, hvis den studerende bryder DSKD´s IT-regler.

8.3. Studietidens ophør

8.3.1. Studietidens ophør

For dimitterende studerende slettes e-mailkonto, når den studerende ikke længere har et aktivt tilhørsforhold til skolen, dog senest 6 måneder efter afslutning på dette.

Ved udmeldelse af skolen deaktiveres e-mailkonto hurtigst muligt.

Studerende har efter studietidens ophør ret til at ansøge om at blive glemt, dvs. få alle data fjernet fra institutionens arkiver, medmindre dette strider mod anden lovgivning. Dog pålægger lovgivningen DSKD at opbevare visse data i længere tid.

9 Styring af ressourcer

DSKD´s IT-afdeling har det overordnede ansvar for implementering og håndtering af ressourcer i overensstemmelse med de nedenfor beskrevne procedurer.

Ressourcer beskriver, det der skal beskyttes, herunder digitale oplysninger, papirdokumenter, fysiske ressourcer som computere og netværk og medarbejderes viden (ISO27001:2013).

9.1 Ansvar for ressourcer

9.1.1 Fortegnelse over ressourcer

Det er IT-afdelingens ansvar, at alle fysiske enheder er registreret med ejer, bruger, serienummer, placering og ibrugtagelsesdato. DSKD´s dataregistre (filer, databaser samt andet personfølsomt materiale) og klassificeres i overensstemmelse med DSKD´s politik for håndtering og sikring af data. Registreringen opdateres løbende af IT-afdelingen (ISO27001:2013).

9.1.2 Ejerskab af ressourcer

IT-afdelingen har ansvar for at udlevere de fysiske ressourcer, dog er det medarbejderens eget ansvar at vedligeholde og passe på disse. Hvert aktiv har en ejer, der er ansvarlig for den løbende opdatering og vedligeholdelse i samråd med IT-afdelingen. IT-afdelingen har ansvar for den overordnede sikkerhed på de anvendte platforme (ISO27001:2013).

9.1.3 Accepteret brug af ressourcer

Alt udleveret udstyr, herunder computere, iPads og telefoner, skal beskyttes med password og/eller fingeraftryk og/eller ansigtsgenkendelse. Udleveret udstyr er strengt personligt og må kun benyttes af medarbejderen. Medarbejderen hæfter for skader påført udstyret af andre, hvis udstyret har været brugt uden for arbejdsmæssig sammenhæng. Det udleverede maskinel må ikke benyttes som host for servere og bit-torrent-programmer. Gældende love og regler forventes overholdt. (ISO27001:2013).

9.1.4 Tilbagelevering af ressourcer

På sidste arbejdsdag tilbageleverer medarbejderen de udleverede informationsressourcer (computer, mobiltelefon, iPads o.l.) samtidig med at adgangen til skolens ressourcer ophæves (jf. afsnit, 3.3.1.

Al tilbageleveret udstyr/enheder formateres, inden der eventuelt skal genudleveres nyt udstyr/enheder (ISO27001:2013).

9.2 Klassifikation af information

5.2.1 Klassifikation af information

DSKD opererer med tre niveauer for klassifikation af informationer:

- **Offentlige**: Materiale, der frit kan udleveres til både interne og eksterne parter uden at fortrolighedsaftaler kræves.
- **Interne**: Materiale, der er tilgængeligt for alle internt i organisationen.
- **(Person)følsomme og fortrolige**: Materiale, der udelukkende er tilgængeligt for en begrænset gruppe personer, for hvem det er relevant.

Med udgangspunkt i de ovenfor angivne niveauer af klassifikation af information vurderer alle medarbejdere, hvorledes data skal behandles og opbevares, og handler derefter.

9.2.2 Håndtering af ressourcer

Medarbejdere med adgang til personfølsomt og fortroligt materiale orienteres om fortrolighed og relevante GDPR-lovgivning (ISO27001:2013).

DSKD har etableret regler og procedurer for overførsel af informationer for alle former for overførselsfaciliteter i DSKD både internt og eksternt samt andre parter (27002:2022, 5.14).

Fortrolige immaterielle ressourcer beskyttes via begrænset adgang.
Fortrolig information må ikke udleveres uden eksisterende aftale med dataejer. Ved udlevering skal gældende lovgivning overholdes.
Fortrolige informationer må ikke efterlades uden opsyn i offentligt tilgængelige rum. Der skaludvises forsigtighed ved omtale af fortrolige informationer i offentlige rum. Al fortroligt materiale skal udskrives som fortroligt print.
Alle medarbejdere er ansvarlige for at beskytte fortroligheden i både egne og kollegaers arbejde – og for at reagere, hvis fortroligheden kompromitteres. Dette gøres ved at kontakte IT-sikkerhed på dpo@dskd.dk (ISO27001:2013).

9.3 Mediehåndtering

5.3.1 Styring af bærbare enheder og udstyr (fx USB-sticks, eksterne harddiske, cd'er).
Udstyr/enheder med fortrolige data må ikke efterlades uden opsyn i offentlige rum eller benyttes på andet udstyr end DSKD´s udstyr.

Ellers gælder de almene regler for klassifikation samt de ovenfor nævnte regler for håndtering af ressourcer (ISO27001:2013).

9.3.2 Bortskaffelse af udstyr/enheder
IT-afdelingen er ansvarlige for at destruere forældede udstyr/enheder, inden de bortskaffes (ISO27001:2013).

9.3.3 Fysiske udstyr/enheder under transport
Fortrolige og/eller personfølsomme data krypteres eller passwordbeskyttes inden transport og afsendelse.

Fysiske medier med fortrolige og/eller personfølsomme data behandles fortroligt under transport og afsendelse.

Der henstilles til, at transport og afsendelse af fortrolige og/eller personfølsomme data begrænses mest muligt (ISO27001:2013).

Digitale udstyr/enheder med fortrolige og/eller personfølsomme oplysninger krypteres eller passwordbeskyttes inden transport eller afsendelse.

Fysiske udstyr/enheder med fortrolige og/eller personfølsomme oplysninger behandles fortroligt under transport og afsendelse (ISO27001:2013).

10 Adgangsstyring

Kun fastansatte medarbejdere og studerende har adgang til at udføre handlinger på DSKD´s IT-systemer, som der er tildelt rettigheder til. Dette styres af IT-afdelingen på baggrund af oplysninger om medarbejdere fra skolens økonomiafdeling samt om studerende fra skolens studieadministration (ISO27001:2013 og ISO27002:2022).

10.1 Forretningsmæssige krav til adgangsstyring

10.1.1 Politik for adgangsstyring

It-afdelingen har det overordnede ansvar for at etablere og vedligeholde procedurer vedrørende adgangsstyring.

Alle brugere skal have unikt brugernavn og bruger-id.

Ved ansættelse af nye medarbejdere tager ansættende leder og IT-afdelingen stilling til, hvilke systemer der skal gives adgang til. Ved omplacering af medarbejdere skal alle rettigheder for den pågældende medarbejder revurderes.

10.1.2 Adgang til netværk og netværkstjenester

Brugere skal kun have adgang til de netværk og netværkstjenester, de er autoriseret til at benytte. Leder og IT-afdelingen tager løbende stilling til, hvilke adgange, der er relevante for den enkelte medarbejder.

Ved ændringer af medarbejderes arbejdsopgaver skal nærmeste leder og IT-afdelingen altid tage stilling til, hvilke adgange, der er relevante for den enkelte medarbejder.

Ved adgangen til det interne netværk fra andre lokationer end Ågade 10, skal der benyttes kodeord og krypteret VPN-forbindelse (ISO27001:2013, ISO27002:2022 og ISO270012023).

10.2 Politik for brugeradgang

10.2.1 Brugerregistrering og –afmelding

Ved ansættelse af ny medarbejder har ansættende leder ansvar for at orientere Økonomi og IT-afdelingen om opstartsdato. Herefter tager ansættende leder og IT-afdeling i fællesskab stilling til, hvilke adgange er relevante for den nye medarbejder. Økonomi udarbejder brugernavn i form af initialer, så der ikke sker sammenfald med andre brugere, og videregiver dette til IT-afdelingen.

Ved ophør af ansættelse har ansættende leder ansvar for at orientere Økonomi og IT-afdelingen om slutdato. Medarbejderen orienteres om procedure for aflevering af hardware (se 4.1.4.). IT-afdelingen sikrer, at medarbejderes adgang til DSKD´s systemer ophører ved ansættelsens udløb, medmindre andet aftales med ansættende leder (ISO27001:2013).

10.2.2. Styring af administrative adgangsrettigheder til hovedsystemer

IT-afdelingen har qua deres ansvarsområder særlige adgange til skolens systemer og servere. Disse administrative adgange skal beskyttes med passwords, som skal følge samme minimumsregler som øvrige password og skal ændres, hvis udenforstående får kendskab til disse, samt hvis systemadministratorers ansættelse ophører.

IT-afdelingen skal sikre, at brugen af disse hovedsystemer begrænses til et minimum af betroede og autoriserede brugere (ISO27001:2022).

10.2.3. Inddragelse eller justering af brugeradgangsrettigheder

Brugeradgangsrettigheder gennemgås af systemejer og IT-afdelingen i forbindelse med nyansættelser, ansættelsesophør samt omrokeringer.

Ved ophør af ansættelse har ansættende leder ansvar for at orientere IT-afdelingen om slutdato. Medarbejderen orienteres om reglerne for aflevering af hardware, (jf. afsnit 8.1.4). IT-afdelingen sikrer, at medarbejderes adgang til DSKD´s systemer ophører ved ansættelsens udløb (ISO27001:2022).

10.2.4 Reparation og vedligeholdelse af udstyr/enheder

I forbindelse med reparation og vedligeholdelse af DSKD´s udleverede udstyr/enheder, kan medarbejder blive bedt om at oplyse sine adgangsoplysninger. Efter endt reparation og/eller vedligeholdelse vil medarbejderen blive bedt om at ændre sit password (ISO27001:2013).

10.2.5 Deling af adgangsoplysninger

I enkelte tilfælde, fx i forbindelse med længevarende sygdom, kan det være hensigtsmæssigt for en medarbejder at dele sine adgangsoplysninger med en anden medarbejder eller at IT-afdelingen kan give adgang ved at resette medarbejderens password. Begge dele skal godkendes af nærmeste leder.

I alle tilfælde, hvor en medarbejder har adgang til en anden medarbejders konto, henstilles der til en skærpet fortrolighed.

Deling af adgangsoplysninger kan også foregå i forbindelse med PA-funktioner. Her aftales de nærmere vilkår og forhold mellem leder og PA under hensyntagen til gældende regler om fortrolighed (ISO27001:2022).

10.2.6 Eksterne underviseres adgang

Som udgangspunkt tildeles eksterne undervisere ikke adgang til skolens systemer med undtagelse af skolens LMS-system og eksamenssystem. Denne adgang tildeles fra studieadministrationen og gives kun til de(t) relevante rum på LMS-systemet.

I enkelte tilfælde kan der være undtagelser for dette, hvis en ekstern underviser har et særligt behov for at kunne tilgå skolens ressourcer. I disse tilfælde er det uddannelseschefens ansvar at sikre, at den eksterne underviser er orienteret om sikker tilgang til skolens ressourcer samt skolens it-sikkerhedspolitik. Det er ligeledes uddannelseschefens ansvar, at studieadministrationen eller IT-afdelingen orienteres, hvis der skal tildeles ekstra adgang til ressourcer (ISO27001:2022).

10.2.7 Reparation og vedligeholdelse af udstyr/enheder

I forbindelse med reparation og vedligeholdelse af DSKD´s udleverede udstyr/enheder, kan medarbejder blive bedt om at oplyse sine adgangsoplysninger. Efter endt reparation og/eller vedligeholdelse vil medarbejderen blive bedt om at ændre sit password (ISO27001:2013).

10.3 Brugernes ansvar

10.3.1 Brug af hemmelig autentifikationsinformation

Password er strengt personlige og må ikke deles med andre, hverken internt eller eksternt i organisationen (se dog undtagelse i 10.2.5). Det er brugerens ansvar at vælge tilstrækkeligt sikre password i adgangskontrolsystemerne (se punkt 10.4.2).

Logning af password i browsere må benyttes, så længe den generelle beskyttelse af computeren med password og/eller biometrisk visning (fx Touch ID, ansigtsgenkendelse) benyttes, og medarbejderen låser computeren, når den ikke er i brug, eller når medarbejderen forlader sin plads (ISO27001:2013, ISO27002:2022 og ISO27001:2023).

10.4 Styring af system- og applikationsadgang

10.4.1 Begrænset adgang til informationer

Adgang til systemer og data styres i overensstemmelse med politikken for brugeradgang (jf. afsnit, 6.1) (ISO27001:2013)

10.3.2 Procedurer for sikre password

Ved brugeroprettelse eller nulstilling af kodeord skal brugere tildeles en sikker, midlertidig adgangskode, som skal ændres umiddelbart efter første anvendelse.

- Kodeord skal være mindst 12 tegn langt.
- Der må ikke benyttes brugernavn, navn eller datoer som en del af kodeord.
- De 5 seneste kodeord opbevares i DSKD´s login-system og kan ikke genbruges.
- Kodeord skal skiftes ved mistanke om misbrug af konto.
- DSKD anvender Authenticator som to-faktor godkendelse for at styrke sikkerheden på DSKD´s konti. Der er nogle undtagelser i hht. bruger uden brugerrettigheder, som er begrænset til kun at have en mail.

(ISO27001:2013).

10.4.3 System for administration af adgangskoder

Ved ansættelse udleveres password af IT-afdelingen. Ved første login udskiftes dette til et personlig password, der overholder ovenstående retningslinjer.

Ved ophør af ansættelse deaktiveres alle personlige password.

Der må ikke installeres tredjeparts-programmer, der kan omgå organisationens fastsatte sikkerhedsprocedurer (ISO27001:2022).

10.4.4 Brug af privilegerede systemprogrammer

Der må ikke installeres tredjeparts-programmer, der kan omgå organisationens fastsatte sikkerhedsprocedurer (ISO27001:2013).

10.4.5 Styring af adgang til kildekoder til programmer

DSKD egenudvikler ikke programmer med kildekode, men benytter godkendte softwarefirmaer som softwareleverandør (ISO27001:2013).

11 Kryptografi

11.1 Politik for anvendelse af kryptering

Alle data på medarbejderes bærbare computere og mobile enheder skal altid beskyttes med password og/eller biometrisk visning (fx Touch ID, ansigtsgenkendelse).

Personfølsomme og fortrolige oplysninger, der sendes via mail, krypteres via Nem-ID/Mit-ID Digital Signatur.

Undtaget herfor er mailkorrespondancer med danske respondenter, som ikke kan modtage krypterede mails. Til disse bruges i stedet e-Boks.

Også undtaget herfor er mailkorrespondancer med udenlandske institutioner, hvor der i stedet indgås databehandlingskontrakter, hvis disse skal modtage personfølsomme eller fortrolige data.

Personfølsomme og fortrolige dokumenter skal opbevares og tilgås på DSKD ´s journaliseringssystem. Store filer eller personfølsomme papirer, der skal sendes til personer udenfor institutionen, kan også sendes via DeiC Filesender, hvortil adgang er beskyttet via WAYF (ISO27001:2022).

11.1.1 Administration af nøgler
DSKD anvender ikke krypteringsnøgler (ISO27001:2013).

12 Fysisk sikkerhed og miljøsikring

Fysisk sikkerhed og adgangsregler for gæster er naturlige elementer i skolens sikkerhedspolitik. Fysisk sikkerhed omfatter blandt andet døre, vinduer, alarmer – samt tyverisikring af skolens fysiske ressourcer, f.eks. it-udstyr. Systemer til adgangskontrol er et naturligt element af skolens sikkerhedspolitik og medvirker til at sikre, at kun personer med legalt ærinde får adgang til skolen (ISO27001:2013, ISO27002:2022 og ISO27001:2023).

12.1 Sikre områder

12.1.1 Fysisk perimetersikring
Alle data hostes på server hostet af ekstern leverandør. Denne eksterne leverandør er ansvarlig for perimetersikring af serverne.

Tilsvarende gælder andre data, når de hostes af eksterne leverandører (Bilag 1, Rollekatalog) (ISO27001:2013 og 27002:2022).

12.1.2 Fysisk adgangskontrol
Adgang til teknikrum og hovedkrydsfelter tillades kun af IT-afdelingen og ejendomsservicetekniker.

Alle krydsfelter og andre teknikrum skal være aflåste (ISO27001:2013).

12.1.3 Sikring af kontorer, lokaler og faciliteter

Alle kontorer aflåses, når de ikke benyttes. Udenfor skolens åbningstider er der kun adgang til skolen via personlige medarbejder- samt studiekort. Medarbejder- og studiekort er personlige og skal opbevares forsvarligt. Bygningens indgangsdøre låses automatisk. Administration af medarbejder- og studiekort samt nøgler til DSKD varetages af skolens ejendomsservicetekniker.

DSKD har videoovervågning på alle ind- og udgange samt udvalgte lokaler. Disse optagelser bruges udelukkende i forhold til opklaring af kriminelle handlinger og opbevares i 14 dage, hvorefter optagelserne slettes automatisk (ISO27001:2013 og ISO27002:2022)

12.1.4 Beskyttelse mod eksterne og miljømæssige trusler

Dataopbevaring er udliciteret til ekstern leverandør, som har ansvaret for sikker og forsvarlig opbevaring, herunder beskyttelse mod diverse trusler (Bilag 1, Rollekatalog) (ISO27001:2013).

12.2 Udstyr

12.2.1 Placering og beskyttelse af udstyr/enheder

Udstyr skal placeres eller beskyttes, så risikoen for skader og uautoriseret adgang minimeres.

Udstyr der benyttes til at behandle kritiske/følsomme informationer skal placeres, så informationerne ikke kan ses af uvedkommende.

Bærbare enheder skal fjernes fra skolens område eller opbevares i aflåste kontorer efter endt arbejdstid (ISO27001:2013).

12.2.2 Understøttende forsyninger (forsyningssikkerhed)

Dataopbevaring er udliciteret til ekstern leverandør, som har ansvar for at sikre de understøttende forsyninger (Bilag 1, Rollekatalog) (ISO27001:2013).

12.2.3 Sikring af kabler

Alle forsyningskabler til netværk er låst inde (ISO27001:2013).

12.2.4 Vedligeholdelse af ressourcer

IT-afdelingen har ansvar for vedligeholdelse af udstyr, efter leverandørens anvisning. Kun godkendte leverandører må udføre reparationer og vedligeholdelse. IT-afdelingen er ansvarlig for at registrere alle fejl og mangler samt reparationer i udstyrsdatabasen (ISO27001:2013).

12.2.5 Fjernelse af ressourcer

Udleveret personligt udstyr/enheder må som udgangspunkt altid medbringes fra skolens område så man kan udføre sin daglige driftsopgaver eller undervisning. Andet udstyr tilknyttet skolen må kun fjernes fra skolens område med tilladelse fra IT-afdelingen. Udlån og fjernelse af disse ressourcer registreres i udstyrs-databasen. Udlån er registreret med tidsbegrænsning. (ISO27001:2013).

12.2.6 Sikring af udstyr og ressourcer uden for organisationen

Alt udstyr er tyverimærket og sikres ved hjælp af password og/eller biometrisk visning (fx Touch ID, ansigtsgenkendelse.

Adgang til skolens data uden for skolens område skal foretages via VPN-adgang (ISO27001:2013).

12.2.7 Sikker bortskaffelse eller genbrug af udstyr

Før udstyr bortskaffes eller genbruges, slettes eller destrueres fysiske harddiske. IT- afdelingen er ansvarlig herfor (ISO27001:2013).

12.2.8 Brugerudstyr uden opsyn

IT-afdelingen har ansvaret for, at udstyr i fællesområder er forsvarligt sikret med fysisk sikring (ISO27001:2013).

12.2.9 Politik for ryddeligt skrivebord og blank skærm

Fortrolige dokumenter fjernes fra skriveborde ved arbejdstid ophør. I løbet af arbejdsdagen vendes dokumenter med blank side opad, hvis skrivebordet forlades. Computerskærme låses, når arbejdsstationen forlades. Disse samme krav til fortrolighed gælder også ved hjemmearbejde (ISO27001:2013).

13 Driftssikkerhed

DSKD´s servere og netværk holdes opdaterede for at sikre det af rektoratet fastsatte ønskede sikkerhedsniveau for skolen.

13.1 Driftsprocedurer og ansvarsområder

IT-afdelingen er ansvarlig for, at alle sikkerhedsregler og procedurer følges i den daglige drift, samt at problemer og fejl opdages, udbedres og rapporteres. IT-afdelingen indgår i det løbende arbejde (forslag

og implementering) med forbedrende sikkerhedstiltag (procedurer, metoder, produkter) (ISO27001:2013).

IT-driften skal planlægges på en sådan måde, at såvel den daglige som den periodiske drift kan afvikles korrekt og til tiden. Driftsplanen skal udarbejdes i tilpas god tid i samarbejde med relevante brugere (ISO27001:2013).

Der skal forefindes relevant, detaljeret og opdateret teknisk netværksdokumentation for DSKD´s lokalnet og eksterne forbindelser. Dokumentationen skal have en detaljeringsgrad og form, så tredjepart (f.eks. konsulenter) vil kunne benytte den i en krisesituation (ISO27001:2013, ISO27002:2022 og ISO27001:2023).

13.1.1 Ændringstyring

Der skal foreligge aktuel driftsdokumentation, der beskriver maskin- og systemmiljøet, samt de forskellige driftsopgaver, manuelle og maskinelle.

IT-driften skal løbende kontrolleres med henblik på hurtig afhjælpning af problemer, fejl og forsinkelser. Kontrollen skal så vidt muligt udføres automatisk.

Større service foregår så vidt muligt uden for almindelig arbejdstid (8.00 – 16.00). For særlige systemer kan der efter aftale med systemejer konkret fastsættes alternative serviceperioder, hvis brugen af systemerne nødvendiggør dette.

Det efterstræbes, at al planlagt nedetid udmeldes så tidligt som muligt, dog mindst 24 timer før. Planlagt nedetid må så vidt muligt ikke forekomme i den almindelig arbejdstid. Undtagelser skal godkendes af administrationschefen (ISO27001:2013).

13.1.2 Kapacitetsstyring

DSKD´s serverdrift styres af ekstern leverandør. Der henvises derfor ved dette punkt til deres politik for kapacitetsstyring (Bilag1, Rollekatalog) (ISO27001:2013).

13.2 Beskyttelse mod malware

13.2.2 Kontroller mod malware

Alle DSKD´s maskiner er udstyret med virusbeskyttelse, der beskytter mod malware. Herudover forudsættes en passende brugerbevidsthed, der understøttes af informationer om malware/phishing fra IT-afdelingen (ISO27001:2013).

13.3 Backup

13.3.1 Backup af information

Da DSKD-servere administreres af en ekstern leverandør, er denne leverandør også ansvarlig for backup af information. DSKD IT-afdeling får dagligt mails med backup-log (Bilag 1, Rollekatalog) (ISO27001:2013).

13.4 Logning og overvågning

13.4.1 Hændelseslogning

DSKD foretager ikke decideret hændelseslogning, men ved hver enkel utilsigtet hændelse foretages en vurdering af, om denne bør forårsage ændringer i procedurer og drift (ISO27001:2013).

13.4.2. Tidssynkronisering

Alle klienter og servere synkroniserer tiden med domæne-kontrolleren (ISO27001:2013).

13.5 Styring af driftssoftware

13.5.1 Softwareinstallation på driftssystemer

IT-afdelingen er ansvarlig for styring og opdatering af softwareinstallation på driftssystemer (ISO27001:2013).

13.6 Sårbarhedsstyring

13.6.1 Styring af tekniske sårbarheder

DSKD orienterer sig om tekniske sårbarheder i institutionens informationssystemer og træffer derudfra beslutninger om eventuelle nødvendige foranstaltninger (ISO27001:2013).

13.6.2 Begrænsninger på softwareinstallation

I og med de maskiner DSKD stiller til rådighed for medarbejderne, er at betragte udelukkende som arbejdsredskaber, henstilles der til den enkelte medarbejder, at arbejdsrelevante apps/programmer vælges med omhu, samt at der udvises sund skepsis i forbindelse med installation af apps/programmer på udleveret udstyr (ISO27001:2013).

13.7 Overvejelser i forbindelse med audit af informationssystemer

13.7.1 Kontroller i forbindelse med audit af informationssystemer

DSKD gennemfører audit af informationssystemer samt verifikation af driftssystemer jævnligt i overensstemmelse med informationssikkerhedspolitikken og på en sådan måde, at det ikke forstyrrer institutionens kerneopgave samt øvrige drift mere end nødvendigt (ISO27001:2013).

14 Kommunikationssikkerhed

14.1 Styring af netværkssikkerhed

14.1.1Netværksstyring

DSKD´s IT-afdeling monitorerer løbende switchene for eventuelle fejl (ISO27001:2013).

14.1.2 Sikring af netværkstjenester

Internetlinjen monitoreres eksternt af internetlinje-leverandøren (ISO27001:2013).

14.1.3 Opdeling af netværk

Netværket er delt op i fem netværk:

- Servicenetværk
- Managementnetværk
- Administrationsnetværk
- Pædagogisk netværk

- Gæstenetværk

Relevante informationstjenester og informationssystemer er tilgængelige på de enkelte netværk (ISO27001:2013).

14.2 Informationsoverførsel

14.2.1 Politikker og procedurer for informationsoverførsel

Personfølsomme og fortrolige data må ikke opbevares eller deles via cloud-baserede storage-tjenester medmindre der som minimum foreligger en databehandleraftale og tjenesten er godkendt af IT-afdelingen. Samtidig skal data forblive i EU.
For øjeblikket er One Drive via Microsoft Office 365 den eneste cloud-baserede løsning, som IT-afdelingen har godkendt.

DSKD holder sig løbende orienteret om EU-kommissionens vurdering af, hvilke lande, der er henholdsvis sikre og usikre at overføre persondata og personfølsomme data til, og handler derefter.

DSKD overfører kun data til databehandler, ikke til dataansvarlige, og er bevidste om institutionens ansvar i at sikre, at disse data behandles i overensstemmelse med Persondataforordningens principper.

I forbindelse med overførelse af persondata samt personfølsomme data til institutioner i tredjepartslande indgår DSKD den af EU-kommissionen forfattede databehandlings-standardkontrakt med disse så vidt muligt. DSKD er opmærksomme på de potentielle sikkerhedsrisici i forbindelse med samarbejder med institutioner i tredjepartslande og følger løbende udviklingen på området og afventer, at EU-kommissionen finder en løsning på problematikken (Bilag 2, Ikke godkendte IT-systemer/software og GDPR).

14.2.2 Aftaler om informationsoverførsel

Ved udveksling af persondata samt personfølsomme data overholdes gældende lovgivning, herunder persondataforordningen.

Ved udveksling af fortrolig information overholdes skolens IT-sikkerhedspolitik (jf. afsnit, 7.1)

Herudover henvises til bilag 2 (Bilag 2, Ikke godkendt IT-systemer og GDPR)

14.2.3 Elektroniske meddelelser

Personfølsomme og fortrolige informationer deles med andre offentlige instanser med kryptering og signering med digital medarbejdersignatur (Mit-ID).

Undtaget herfor er mailkorrespondancer med danske respondenter, som ikke kan modtage krypterede mails. Til disse bruges i stedet e-Boks.

Også undtaget herfor er mailkorrespondancer med udenlandske institutioner, hvor der i stedet indgås databehandlingskontrakter, hvis disse skal modtage personfølsomme eller fortrolige data. Store filer eller personfølsomme papirer, der skal sendes til personer udenfor institutionen, kan også sendes via DeiC Filesender, hvortil adgang er beskyttet via WAYF.

14.2.4 Fortroligheds- og hemmeligholdelsesaftaler

DSKD opererer med tre niveauer for klassifikation af informationer:

- Offentlige: Materiale, der frit kan udleveres til både interne og eksterne parter uden at fortrolighedsaftaler kræves.
- Interne: Materiale, der er tilgængeligt for alle internt i organisationen.
- (Person)følsomme og fortrolige: Materiale, der udelukkende er tilgængeligt for en begrænset gruppe personer, for hvem det er relevant.

Det er rektoratets og ledelsens ansvar at informere medarbejdergruppen om gældende lovgivning, herunder Persondataforordningen, samt skolens informationssikkerhedspolitik. Det er den enkelte medarbejders ansvar at være opmærksom på, at fortrolige og personfølsomme data ikke deles via ikke-sikre kommunikationsformer.

Der henstilles til generel årvågenhed over, hvad der deles via e-mails, sociale medier m.v.

15 Anskaffelse, udvikling og vedligeholdelse af systemer

15.1 Sikkerhedskrav til informationssystemer

15.1.1 Analyse og specifikation af informationssikkerhedskrav

Det er IT-afdelingens ansvar at sikre, at skolens interne IT-systemer er sikkerhedsmæssigt forsvarlige og supporteres af hardware og softwareudbydere. Samtidig skal IT-afdelingen holde sig løbende opdaterede om udviklingen, så de er informerede om evt. sikkerhedsproblematikker.

15.1.2 Sikker systemarkitektur og udviklingsprincipper
DSKD udvikler løbende principper, der sikrer IT-systemerne udvikles, vedligeholdes, dokumenteres og anvendes i forbindelse med informationssystemerne. Dette er for at sikre at informationssystemerne tilrettelægges, implementeres og betjenes sikkert i dens udviklingscyklus (ISO27002:2022, 8.27)

15.1.3 Sikkerhedstest under udvikling og godkendelse
DSKD har agil projektstyring og har derved processor til sikkerhedstest som defineres og implementeres i udviklingslivscyklen. Dette er for at validere om informationssystemerne lever op til de informationssikkerhedskrav der er når nye IT-systemer, software og lignende implementeres i DSKD´s systemlandskab (ISO:2022, 8.29).

15.1.4 Ændringsstyring
DSKD sikrer vha. ændringsstyring, at informationsbehandlingsfaciliteter og informationssystemer er underlagt faste procedure for at bevare informationssikkerheden ved udførsel af ændringer (ISO27002:2022, 8.32).

15.1.5 Sikring af applikationstjenester på offentlige netværk
Der henstilles til den enkelte medarbejder, at apps/programmer vælges med omhu, samt at der udvises sund skepsis i forbindelse med installation af sådanne apps/programmer på udleveret udstyr.

Ved opståede fejl vil IT-afdelingen være behjælpelige med at føre det udleverede udstyr tilbage til standardinstallation.

Ved mistænkelige hændelser rettes henvendelse til IT-afdelingen.

15.1.6 Beskyttelse af handelsapplikationer og –tjenester
For at beskytte informationer i forbindelse med overførsler af handelsapplikationer og tjenester er al tilgang til digitale butikker beskyttet med password og/eller biometrisk visning (fx Touch ID, ansigtsgenkendelse).

15.2 Sikkerhed i udviklings- og hjælpeprocesser

DSKD udvikler ikke selv software og systemer og anvender kun standardiseret software.

15.3 Testdata

DSKD udvikler ikke selv software og systemer og anvender kun standardiseret og godkendt software.

16 Leverandørforhold

16.1 Informationssikkerhed i leverandørforhold

16.1.1 Informationssikkerhedspolitik for leverandørforhold

Ved indgåelse af aftaler med eksterne leverandører specificeres, hvilke data m.v. leverandøren har adgang til, samt at leverandøren forpligter sig til at overholde persondataforordningen ved behandling, opbevaring og eventuel videregivelse af data. Relevante forhold vedrørende personfølsomme og/eller fortrolige oplysninger samt forhold omfattet af tavshedspligt skal fremgå af aftalerne med eksterne samarbejdspartnere.

Kravene til IT- og informationssikkerhed og behandling af personfølsomme data beskrives således i de aftaler, der indgås med de eksterne samarbejdspartnere, f.eks. i databehandleraftaler.

DSKD´s netværksleverandører skal i henhold til det aftalte kunne levere:

- De nødvendige teknologiske muligheder for autentifikation og kryptering
- De nødvendige tekniske opsætninger til at sikre opkoblinger i overensstemmelse med samarbejdsaftalen
- Adgangskontrol der sikrer mod uvedkommendes adgang
- Overholdelse af DSKD´s til enhver tid gældende Informationssikkerhedspolitik samt lovgivning, herunder Persondataforordningen.

17 Styring af IT- og informationssikkerhedsbrud

17.1.1 Styring af IT- og informationssikkerhedsbrud samt forbedringer

Ved konstatering af brud eller formodede brud på it-sikringsforanstaltninger, herunder ukendte e-mails, e-mails med ejendommelige overskrifter og fejlbehæftet sprog, dobbelt sign-on hjemmesider, snydetelefonopkald, samt alt andet, der virker påfaldende, skal rapportering straks ske til it-afdelingen, som herefter vurderer informationssikkerhedsbruddets grovhed. Dette gælder både for interne medarbejdere og eksterne leverandører.

I tilfælde af alvorlige informationssikkerhedsbrud afrapporterer IT-afdelingen omgående til informationssikkerhedskoordinatoren, der herefter tager stilling til, om bruddet er så alvorligt, at rektoratet skal inddrages.

Brud på sikkerheden, uautoriseret adgang og forsøg på uautoriseret adgang til systemer, informationer og data skal registreres. Hvis et sikkerhedsbrud afstedkommer et retsligt efterspil uanset om sikkerhedsbruddet er foretaget af en person eller en virksomhed, så skal der indsamles, opbevares og præsenteres et fyldestgørende bevismateriale.

Når en sag vedrørende informationssikkerhedsbrud er afsluttet, foretager IT-afdelingen foranstaltninger, der så vidt muligt sikrer, at et tilsvarende brud ikke sker en anden gang.

17.1.2 Underretning om trusler

DSKD tager cyberkriminalitet alvorligt og tager derfor stilling til DSKD´s trusselsbillede i de forskellige aspekter. Dette har til formål at skabe målrettet beredskabsplaner og sikre størst tryghed blandt alle DSKD´s interessenter samt være forberedte på, hvis der skulle være et cyberangreb på DSKD (27002:2022, 5.7)

17.1.3 Planlægning og forberedelse af incidenthåndtering ved sikkerhedsincidents

DSKD har klarlagt og forberedt sig på at håndtere informationssikkerheds incidents ved at definere, etablere og kommunikere processer, roller og ansvar for styring af informationssikkerheds incidents (27002:2022, 5.24).

17.1.4 Vurdering af og beslutning om informationssikkerhedshændelser

Ved sikkerhedshændelser vurderer DSKD, hvor vidt disse er kategoriseret som informationssikkerheds incidents (27002:2022, 5.25).

17.1.5 Styring af persondatasikkerhedsbrud og forbedringer

Hvis en medarbejder konstaterer et brud på persondatasikkerheden, kontaktes IT-sikkerhedsudvalget, som herefter vurderer bruddets alvor, herunder om dette kan indebære en risiko for fysiske personers rettigheder eller frihedsrettigheder, og orienterer dataejer, nærmeste leder, rektor samt DPO, alt efter hvad der vurderes relevant i forhold til bruddets alvor. (Jf. 19.1.3. Privatlivets fred og beskyttelse af personoplysninger)

Hvis et brud indebærer en risiko, skal bruddet uden unødvendig forsinkelse og senest 72 timer efter det er blevet opdaget, anmeldes til Datatilsynet, samtidig med at dataejer og DPO informeres.

Ved alvorlige og/eller forsætlige brud på persondatasikkerheden orienterer dataejer og nærmeste leder rektoratet, som tager stilling til eventuelle konsekvenser, herunder forbedring af systemer, så sådanne brud ikke gentages.

Når en sag vedrørende persondatasikkerhedsbrud er afsluttet, foretager IT-sikkerhed i samarbejde med dataejer foranstaltninger, der så vidt muligt sikrer, at et tilsvarende brud ikke sker en anden gang.

18 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

DSKD har udliciteret opbevaring af data m.v. Serverrum og sikring af dette er således omfattet af den eksterne leverandørs IT- og informationssikkerhedspolitik og beredskab, som DSKD er bekendt med.

Elektronisk post opbevares i Microsofts cloud-baserede posttjeneste. Dertil kommer, at visse data vedrørende de studerende opbevares hos STADS, samt at DSKD´s bogholderi benytter økonomistyringssystemet Navision, hvori data derfor også opbevares.

Internt opbevares alt personfølsomme og fortrolige data i et dokumenthåndteringssystem (ESDH).

DSKD´s IT-afdeling er ansvarlig for at vedligeholde og ajourføre en systemejer-oversigt. Systemejerne er ansvarlige for at identificere kritiske processer.

IT-afdelingen er ansvarlig for at kontakte serviceudbyder i forbindelse med nedbrud af et eller flere systemer og i samarbejde med denne få systemerne tilbage til normal drift. IT-afdelingen er ligeledes ansvarlig for at informere medarbejdere om tidsestimat for genoptagelse af den normale drift.

18.1 Redundans

Sikring af data foretages af SDU og er beskrevet i deres informationssikkerhedspolitik. IT-linjer mellem DSKD og SDU er af økonomiske årsager ikke redundante, men de fleste af DSKD´s funktioner vil kunne foretages af medarbejderne fra eksterne internetforbindelser.

19 Overensstemmelse

19.1 Overensstemmelse med lov- og kontraktkrav

19.1.1 Identifikation af gældende lovgivning og kontraktkrav

Rektoratet har ansvaret for at identificere lovgivning, der er relevant for DSKD´s drift, eller udpege en person der er ansvarlig for denne opgave. Rektoratet er ansvarlig for at alle eksterne sikkerhedskrav og DSKD´s håndtering heraf, klarlægges, dokumenteres og løbende vedligeholdes

19.1.2 Immaterielle rettigheder

Rektoratet har det overordnede ansvar for, at DSKD fastholder en

nødvendig opmærksomhed på ikke at krænke tredje parts ophavsrettigheder.

IT-afdelingen skal vedligeholde dokumentation for ejendomsretten af licenser.

IT-afdelingen skal løbende kontrollere, at software-licensaftaler overholdes, f.eks. at eventuelle begrænsninger i antal brugere, servere eller kopier overholdes.

IT-afdelingen skal løbende kontrollere, at der kun er installeret autoriserede systemer med autoriserede licenser på udstyr udleveret af DSKD.

Registrering af softwarelicenser sker gennem IT-afdelingen. Det er IT-afdelingensoverordnede ansvar, at der er et tilstrækkeligt antal licenser.

Medarbejdere må ikke forpligte DSKD ved at acceptere licensvilkår i software, som ikke er forhåndsgodkendt af IT-afdelingen.

Ansatte må ikke kopiere, konvertere eller udtrække information fra billed- og lydfiler eller tilsvarende ressourcer, med mindre dette specifikt tillades fra rettighedshaveren.

Ansatte må ikke kopiere bøger, artikler, rapporter eller andre dokumenter, helt eller delvist, med mindre dette specifikt tillades fra rettighedshaveren.

19.1.3 Privatlivets fred og beskyttelse af personoplysninger

I alle sammenhænge, herunder både i forhold til skolens kerneopgave som uddannelsesinstitution samt intern og ekstern kommunikation, bestræber DSKD sig på at respektere privatlivets fred samt overholde den til enhver tid gældende lovgivning, herunder Persondataforordningen.

Hvis en medarbejder konstaterer et brud på persondatasikkerheden, har medarbejderen ansvar for at orientere IT-sikkerhedsgruppen om dette brud. Denne orientering skal altid foregå på mail DPO@dskd.dk, men derudover har medarbejderen ansvaret for at sikre, at IT-sikkerhedsgruppen modtager denne orientering, fx i ferieperioder.

IT-sikkerhedsgruppen tager herefter stilling til bruddets alvor, herunder om dette kan indebære en risiko for fysiske personers rettigheder eller frihedsrettigheder, og orienterer dataejer, nærmeste leder og skolens rektorat samt DPO, hvis det vurderes nødvendigt.

Hvis et brud indebærer en risiko, skal IT-sikkerhedsudvalget uden unødvendig forsinkelse og senest 72 timer efter at denne er blevet bekendt med bruddet, anmelde dette til Datatilsynet.

Ved alvorlige og/eller forsætlige brud på persondatasikkerheden orienterer dataejer og nærmeste leder rektoratet, som tager stilling til eventuelle konsekvenser, herunder forbedring af systemer, så sådanne brud ikke gentages.

Når en sag vedrørende persondatasikkerhedsbrud er afsluttet, foretager dataejer foranstaltninger, der så vidt muligt sikrer, at et tilsvarende brud ikke sker en anden gang.

Personoplysninger af fortrolig karakter må kun behandles på mobilt udstyr, hvis dette er password-beskyttet og/eller beskyttet med fingeraftryk og/eller ansigtsgenkendelse, eller disse oplysninger tilgås via VPN-forbindelse.

Ledelsen skal sikre, at medarbejdere informeres om eventuelle overvågningsmuligheder, som DSKD kan tage i brug, herunder netværksovervågning ved mistanke om misbrug (Bilag 3, Procedure for IT-sikkerhedsbrud).

19.1.4 Regulering af kryptering

DSKD skal efterleve de nationale regler for kryptering. DSKD krypterer post, der sendes til styrelser og andre myndigheder via NemID/Mit-ID.

Undtaget herfor er mailkorrespondancer med danske respondenter, som ikke kan modtage krypterede mails. Til disse bruges i stedet e-Boks.
Også undtaget herfor er mailkorrespondancer med udenlandske institutioner, hvor der i stedet indgås databehandlingskontrakter, hvis disse skal modtage personfølsomme eller fortrolige data.
Rektoratet og den informationssikkerhedsansvarlige er ansvarlige for at informere medarbejdere om de regler og retningslinjer, der er gældende vedr. udveksling af personfølsomme data.

19.2 Gennemgang af informationssikkerhed

19.2.1 Uafhængig gennemgang af informationssikkerhed
Som netværksudbyder er den eksterne leverandør ansvarlig for sikkerhedsniveauet i interne og eksterne netværksudstyr og servere (Bilag 1, Rollekatalog).

Det er ikke tilladt at forsøge at omgå sikkerhedsmekanismer.

Det er ikke tilladt at foretage uautoriseret afprøvning af sikkerheden.

Bevidste eller gentagne overtrædelser kan medføre, at ansættelses- eller samarbejdsforholdet overvejes fra DSKD´s side.

Hændelser, hvor medarbejdere er involverede, bliver håndteret i overensstemmelse med gældende personalepolitik.

Det er rektoratets ansvar, at sanktioner for brud på DSKDs politikker, regler eller retningslinjer håndhæves i overensstemmelse med gældende lovgivning.

19.2.2. Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder
Rektoratet skal regelmæssigt sikre, om informationsbehandlingen og -procedurerne inden for IT-området er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav.

19.2.3. Undersøgelse af teknisk overensstemmelse
IT-afdelingen er ansvarlig for at sikre regelmæssige undersøgelser af, at skolens forskellige systemer er i overensstemmelse med DSKD´s informationssikkerhedspolitikker og standarder.

20. Individets rettigheder

DSKD tilstræber at behandle så få personoplysninger om medarbejdere, studerende og andre samarbejdspartnere som muligt, ligesom der kun foretages en behandling af personoplysninger, hvis behandlingen er nødvendig og sagligt begrundet.

20.1. Procedure for indsamling af personoplysninger

Som uddannelsesinstitution indsamler **DSKD** personoplysninger om flere kategorier af personer:

- Ansøgere til uddannelsen
- Optagne og indskrevne studerende
- Udvekslingsstuderende
- Kursister på efteruddannelsen
- Ansatte
- Eksterne undervisere
- Samarbejdspartnere
- Brugere – fx i forbindelse med empiriindsamling
- Gæster i huset

I nogle af disse tilfælde modtager DSKD data fra andre institutioner eller offentlige myndigheder, fx i forbindelse med optagelse gennem Den Koordinerede Tilmelding. I andre tilfælde indleverer personer selv data, fx i forbindelse med studerendes ansøgning om orlov.

Fælles for alle disse er, at DSKD ikke indhenter flere oplysninger end nødvendigt – det er derfor forskelligt, hvilke kategorier af personoplysninger vi har om de forskellige kategorier af registrerede personer. Alle persondata opbevares forsvarligt som beskrevet tidligere i denne it- og informationssikkerhedspolitik.

DSKD er dataansvarlig for alle indsamlede data.

I øvrigt gælder nedenstående procedurer for de data, skolen har indhentet.

20.2. Procedure for gennemsigtighed og indsigtsret

Medarbejdere giver i forbindelse med tiltrædelsen lov til, at DSKD under ansættelsen opbevarer og behandler deres data og informationer. Disse data og informationer opbevares fortroligt og deles kun med offentlige myndigheder efter aftale med medarbejderen, fx i forbindelse med sygdom. DSKD deler ikke medarbejderdata med tredjepart.

Alle medarbejdere har til enhver tid ret til at få oplyst, hvilke data institutionen ligger inde med om vedkommende. Disse data vil blive gjort tilgængelige for medarbejderen indenfor 14 dage.

For skolens studerende, dimittender, eksterne undervisere og eksterne med løs eller ophørt tilknytning til skolen gælder tilsvarende, at de har ret til at få oplyst, hvilke data institutionen ligger inde med, og at disse vil blive gjort tilgængelige indenfor 14 dage.

Af hensyn til positiv identifikation af ansøger skal henvendelser fremsendes via E-boks/Digital Postkasse eller ansøger skal møde op på skolen og positivt identificere sig selv med gyldigt billede-ID.

20.3. Procedure for berigtigelse

DSKD bestræber sig på, at alle personoplysninger er rigtige og ajourførte.

Enhver med tilknytning til skolen har ret til og krav på at kunne berigtige de informationer, som skolen ligger inde med.

Henvendelse om berigtigelse fremsendes skriftligt til skolen.

Af hensyn til positiv identifikation af ansøger skal henvendelser fremsendes via E-Boks/Digital Postkasse eller ansøger skal møde op på skolen og positivt identificere sig selv med gyldigt billede-ID.

I tilfælde af mindre uoverensstemmelser som fx stave- eller tastefejl i forbindelse med faktiske personoplysninger korrigeres disse hurtigst muligt, og berigtigelsen meddeles til den berørte.

Hvis det derimod drejer sig om større uoverensstemmelser skal disse dokumenteres. Dokumentationen skal indeholde oplysninger både om, hvad der skal berigtiges, hvad der bliver berigtiget til samt sagsforløbet.

Dokumentationen opbevares i skolens dokumenthåndteringssystem samt formidles til den berørte.

20.4. Procedure for sletning og tilbagetrækning af samtykke (retten til at blive glemt)

DSKD er som offentlig myndighed underlagt love og bestemmelser, der i visse situationer står over GDPR-lovgivningen. I situationer hvor personer henvender sig til skolen om at få trække deres samtykke tilbage eller få deres personoplysninger slettet, vil skolen naturligvis efterkomme dette, hvis det ikke strider mod anden lovgivning.

En af skolen registreret person har til enhver tid ret til at trække sit samtykke tilbage, hvorefter skolen hurtigst muligt skal ophøre med at behandle det af samtykket omfattede.

Det er ikke muligt at trække samtykke tilbage, hvor der er en kontraktlig aftale eller anden lovgivning.

Henvendelse om tilbagetrækning af samtykke fremsendes skriftligt til skolen, hvorefter skolen behandler denne hurtigst muligt uden unødig forsinkelse under hensyntagen til gældende lovgivning.

DSKD er opmærksom på, at behandling også omfatter opbevaring og vil efter ønske om tilbagetrækning af samtykke slette og/eller destruere det af samtykket omfattede under hensyntagen til øvrig lovgivning.

Henvendelse om sletning fremsendes skriftlig til skolen.

Af hensyn til positiv identifikation af ansøger skal henvendelser fremsendes via e-Boks eller ansøger skal møde op på skolen og positivt identificere sig selv med gyldigt billede-ID.

Ved henvendelse undersøger skolen, hvilke informationer man ligger inde med om ansøger. Herefter vurderer skolen i hvilket omfang denne sletning kan udføres under gældende lovgivning. Hvis skolen har hjemmel til at udføre sletning, vil denne foregå indenfor en måned efter fremsendt henvendelse om sletning.

Dokumentation for sletning fremsendes til ansøger.

20.5. Procedure for begrænsning

Enhver person med tilknytning til DSKD har ret til at begrænse adgangen til sine personoplysninger, så skolen ikke foretager andet end opbevaring af disse.

Denne ret gælder, hvis en af følgende forudsætninger er opfyldt:

1. Hvis person mener, at personoplysninger er ukorrekte (se 20.2. Berigtigelse).
2. Hvis skolen behandler personoplysninger ulovligt, men personen ikke ønsker dem slettet.
3. Personoplysningerne er ikke nødvendige til behandling, men er nødvendige i forhold til et retskrav.
4. Hvis personen gør indsigelser mod behandlingen.

I tilfælde hvor en person anmoder om begrænsning, oprettes en mappe ved navn 'Begrænsning' i skolens dokumenthåndteringssystem, hvor disse data overføres til.

Henvendelse om begrænsning fremsendes skriftlig til skolen.

Af hensyn til positiv identifikation af ansøger skal henvendelser fremsendes via e-Boks eller ansøger skal møde op på skolen og positivt identificere sig selv med gyldigt billed-id.

20.6. Dataportabilitet

DSKD opbevarer kun persondata og personfølsomme data i standardformater og anvender alment benyttede IT-systemer til at registrere og opbevare data.

I tilfælde hvor registrerede personer ønsker at modtage egne personoplysninger eller overføre personoplysninger fra DSKD til en anden dataansvarlig, rettes der skriftlig henvendelse til skolen, hvorefter skolen behandler denne hurtigst muligt uden unødig forsinkelse.

Af hensyn til positiv identifikation af ansøger skal henvendelser fremsendes via e-boks eller ansøger skal møde op på skolen og positivt identificere sig selv med gyldigt billede-ID.

21. Brug af billeder

Hvis du bruger billeder af personer, skal du være opmærksom på, at Datatilsynet anser offentliggørelsen af billeder på internettet for en behandling af personoplysninger. Etbillede med andre personer er derfor oplysninger om disse personer.
Datatilsynet sondrer ikke længere mellem situationsbilleder og portrætbilleder. Desuden har datatilsynet ikke nedskrevne regler for video, men her bør du følge reglerne for billeder.
Man skal derfor leve op til databeskyttelsesreglerne, når man offentliggør billeder påinternettet.

Hvis du selv tager billeder og optager video af personer til brug på DSKD´s platforme, skal du være opmærksom på, at du er omfattet af databeskyttelsesreglerne og – forordningen. Du skal derfor sørge for, at du har ret til at offentliggøre og/eller opbevare billeder/video, fx fordi du har fået samtykke fra personen.

På Designskolens medieserver kan du sikkert gemme alle dine arbejdsmæssige videoer, billeder og lydoptagelser. Her kan du gemme medier med persondata sikkert og forsvarligt.Du bestemmer, hvem du deler dine filer med, og de er sikkert opbevaret på sikre servere i Danmark. Du finder mere info i bilag 6 (bilag 6, Data typer og håndtering her af)

21.2. DSKD´s billedpolitik

1. Alle billeder og videoer med genkendelige personer fra før 2017 skal slettes fra offentlige kanaler og må ikke bruges fremadrettet – medmindre der foreligger beviseligt tilsagn fra de portrætterede personer
2. Fra årgangene med studiestart 2017-2020 har alle studerende underskrevet tilsagn om, at vi må bruge deres billeder – både i kommunikation- og administrativ sammenhæng. Disse må derfor gerne benyttes til både ekstern og intern kommunikation. For studerende optaget med studiestart 2021 og frem skal forelægge dokumentation for tilsagn ved brug af billeder til kommunikation og i administrative sammenhænge.
3. Hvis studerende ikke giver tilsagn til, at vi må bruge deres billeder, må vi ikke.
4. For alle eksterne samarbejdspartnere, studerende på diplomuddannelsen og i det hele taget på efter- og videreuddannelsen skal der foreligge beviseligt tilsagn fra de portrætterede personer.
5. Hvis de portrætterede er offentlige personer i det offentlige rum, må billederne gerne bruges til både ekstern og intern kommunikation.
6. Hvis de portrætterede er almindelige mennesker, der deltager i et arrangement på skolen, skal de spørges, om de ønsker deres billede taget og delt. Dette gælder alle situationer, hvor de portrætterede personer kan blive identificeret.

Bilag

Bilag 1: Rollekatalog

Bilag 2: Ikke godkendte IT-systemer/software og GDPR

Bilag 3: Procedure for IT-sikkerhedsbrud

Bilag 4: Retningslinjer for video-møder

Bilag 5: Brug af udlånt mobiltelefon

Bilag 6: Data typer og håndtering her af

Brug af billeder og video med personer

Hvis du offentliggør billeder af personer, skal du være opmærksom på, at Datatilsynet normalt anser det for en behandling af personoplysninger, og du skal derfor leve op til databeskyttelsesreglerne.

Datatilsynet sondrer ikke længere mellem situationsbilleder og portrætbilleder. Desuden har Datatilsynet ikke nedskrevne regler for video, men her bør du følge reglerne for billeder.

Man skal derfor leve op til databeskyttelsesreglerne, når man offentliggør billeder på internettet.

Vigtige overvejelser

Inden offentliggørelse af et billede, skal du have styr på følgende:

A. Samtykke eller hjemmel?

Du skal have et grundlag for at offentliggøre et billede med personer på, fx samtykke

eller lovhjemmel, fordi offentliggørelsen udgør et naturligt led i de opgaver, som universitetet

skal varetage iflg. lovgivningen.

Vurder nøje, om du har brug for et samtykke fra personen på billedet.

Det afgørende for, om du må bruge et billede uden tilladelse er, at personerne på billedet ikke

føler sig udstillede eller udnyttede. Dette er en vurderingssag, og er du blot en smule i tvivl, bør

du få en tilladelse fra personerne på billeder, før du offentliggør det.

B. Orienter om offentliggørelse

Hvis du vil offentliggøre et billede uden først at have indhentet samtykke, skal du stadig sikre dig, at den eller de personer, der er på billedet, er vidende om, at du har tænkt dig at offentliggøre billedet på internettet, så de har mulighed for at reagere, fx gøre indsigelse imod det.
Som eksempel kan du til konferencer og arrangementer orientere om, at der bliver taget billeder, og at en række af disse billeder vil blive anvendt til at fortælle om arrangementet eller et lignende arrangement. Du kan orientere ved at skrive informationen ind i programmet, lægge en flyer frem, hvor det står på, skrive det på en storskærm eller lignende. Du skal huske at informere deltagerne om deres rettigheder.

C. Korrekt sammenhæng

Du skal nøje vurdere, om billedet bliver brugt i den sammenhæng, som det er tænkt ind i. Det betyder også, at billedet ikke må være for gammelt.

Det offentlige rum

Billeder der er taget i det offentlige rum, det kan være på gader, i parker og andre steder, hvor der ikke er nogen adgangsbegrænsning. De billeder må du offentliggøre, under hensyntagen til visse kriterier. (Der kan være opstillet betingelser for fotografering i offentlige områder, f.eks. retsbygninger, lufthavne, metro, storcentre, banegårde mv.) Man kan som udgangspunkt ikke altid være sikker på, at man må tage billeder på offentlig grund. Brug sund fornuft.
Det afgørende kriterium i forbindelse med vurdering af eventuel offentliggørelse er, at den afbildede ikke med rimelighed må kunne føle sig udstillet, udnyttet eller krænket, f.eks. i markedsførings eller andet kommercielt øjemed. Billederne skal med andre ord være

harmløse ud fra en normal betragtning.

Billeder kan dog være af en sådan beskaffenhed, at det må antages at virke krænkende for de afbildede. Dette kunne f.eks. være hvis to genkendelige personer bliver afbildet i intime situationer, folk der nøgenbader, folk der skændtes, eller genkendelige personer der har været udsat for en trafikulykke.

Følgende situationsbilleder vil normalt ikke kunne offentliggøres uden samtykke:

- Personbilleder der er taget steder, hvor der ikke er offentlig adgang kan f.eks. være i et privat hjem eller inde i en bil. Her må du ikke tage billeder af personer, som befinder sig på dette område, uden deres samtykke.
- Personbilleder der er taget af ansatte på deres arbejde i en privat virksomhed eller hos en offentlig myndighed.
- Billeder taget til private arrangementer og sammenkomster, kræver at alle der kan identificeres på billedet, skal give samtykke.
- Billeder af kunder i en forretning, i banken, på posthuse, gæster på et diskotek mm.
- Billeder af besøgende hos lægen, kunder i banken eller lignende. Billedet indeholder personer med strafbare forhold.
- Billedet indeholder følsomme oplysninger om de eller den person på billedet.

Bemærk: Du må gerne offentliggøre et krænkende billede - du må bare ikke kunne identificere personen eller personerne på billedet. Man ser det ofte med personbilleder, hvor der er indsat en sort bjælke over ansigtet, eller billedet er taget af personen bagfra, så man ikke kan identificere personen.

Sikker opbevaring af video, billeder og lyd

På Designskolens medie-server kan du sikkert gemme alle dine arbejdsmæssige videoer, billeder og lydoptagelser. Her kan du gemme medier med persondata sikkert og forsvarligt. Du bestemmer, hvem du deler dine filer med, og de er sikkert opbevaret på sikre servere i Danmark.

Tager du selv billeder og optager video?

Hvis du selv tager billeder og optager video af personer til brug på DSKDs platforme, skal du være opmærksom på, at du er omfattet af databeskyttelsesreglerne og –forordningen. Du skal derfor sørge for, at du har ret til at offentliggøre og/eller opbevare billeder/video, fx fordi du har fået samtykke fra personen.

Samtykke

En samtykkeerklæring er en erklæring, hvor den portrætterede person giver billedetageren ret til at anvende billedet på forskellige medier. Et samtykke kan gives mundtligt eller skriftligt. Det er dog billedetageren, virksomheden eller organisationen, der skal bevise, at der i den konkrete situation er afgivet samtykke, og at det i øvrigt lever op til persondatalovens krav til et samtykke.

Krav til en samtykkeerklæring:

Samtykket skal være frivilligt

Når et samtykke skal være *frivilligt* betyder det, at der ikke må hæftes krav eller betingelser om samtykke sammen med fx levering af en ydelse eller køb af varer.

- Du må altså ikke kræve samtykke til fx at modtage reklamer, nyhedsbreve eller anden behandling af en persons data, for at denne person kan få lov til at købe en vare.
- Det må således ikke være afgivet under tvang.
- I nogle tilfælde kan der dog herske tvivl om frivilligheden, da der kan forekomme modydelser for at meddele samtykket.

Samtykket skal være specifikt og informeret

- At et samtykke skal være **specifikt** betyder, at du giver samtykke til behandling med et bestemt formål, ikke et bredt samtykke, som kan fortolkes som virksomheden ønsker det, eller som dækker mange forskellige formål.

- Samtykket skal være **informeret**, hvilket betyder, at den registrerede er informeret om, hvad samtykket vil betyde for kunden, fx at vedkommende bliver genstand for målrettet markedsføring.
- Dette må under ingen omstændigheder skjules i anden tekst.

Samtykket skal være utvetydigt & udtrykkeligt

- Samtykket skal være **utvetydigt**. Man må altså ikke være i tvivl om, at der er givet samtykke, og der skal derfor udføres en aktiv handling fra fx kundens side, såsom at sætte flueben i en boks eller udfylde en blanket.
- Samtykke skal være **udtrykkeligt**. Det betyder, at der skal være tale om en aktiv handling fra den registreredes side.

Det er altså ikke godt nok, hvis man skriver eller siger til personen, at hvis han/hun ikke protesterer inden f.eks. en uge, går man ud fra, at der foreligger et samtykke.

Billeder med børn

Når det skal vurderes, om offentliggørelsen af et billede med børn og unge er lovlig, skal man tænke på, at børn skal gives en særlig beskyttelse. Fordi de oftest er mindre bevidste om de risici og konsekvenser, som kan være forbundet med behandling af personoplysninger.

Hvis du har givet dit samtykke til en billedetager, virksomhed eller organisation, kan du til enhver tid trækker den tilbage. Ved at kontakte den billedetager, virksomhed eller organisation, der har indhentet den, -også selvom der er tale om lovlige billeder. Husk på at et samtykke ikke er tidsbegrænset, det løber indtil det bliver trukket tilbage. Der kan ikke tilbagekaldes samtykke med tilbagevirkende kraft.

Tilbagekaldelse af samtykke

De personer der er portrætteret, kan til enhver tid gøre indsigelse. De skal i så fald oplyse, hvilket billede der ønskes slettet og hvorfor. Hvis en eller flere personer, der er på billedet, ikke ønsker at have billedet liggende på internettet, bør det umiddelbart fjernes af den

dataansvarlige.

Hvis den dataansvarlige ikke vil imødekomme anmodningen om at slette billedet, kan vedkommende klager til Datatilsynet.

Billedpolitik i punkform

1. Alle billeder og videoer med genkendelige personer fra før 2017 skal slettes fra offentlige kanaler og må ikke bruges fremadrettet – medmindre der foreligger beviseligt tilsagn fra de portrætterede personer.
2. Fra årgangene med studiestart 2017-2020 har alle studerende underskrevet tilsagn om, at vi må bruge deres billeder – både i kommunikation- og administrativ sammenhæng. Disse må derfor gerne benyttes til både ekstern og intern kommunikation. For studerende optaget med studiestart 2021 og frem skal forelægge dokumentation for tilsagn ved brug af billeder til kommunikation og i administrative sammenhænge.
3. Hvis studerende ikke giver tilsagn til, at vi må bruge deres billeder, må vi ikke.
4. For alle eksterne samarbejdspartnere, studerende på diplomuddannelsen og i det hele taget på efter- og videreuddannelsen skal der foreligge beviseligt tilsagn fra de portrætterede personer.
5. Hvis de portrætterede er offentlige personer i det offentlige rum, må billederne gerne bruges til både ekstern og intern kommunikation.
6. Hvis de portrætterede er almindelige mennesker, der deltager i et arrangement på skolen, har de ret til at blive spurgt, om de ønsker deres billede delt. Dette gælder alle situationer, hvor de portrætterede personer kan blive identificeret.