Politikker for persondata og data-beskyttelse

Godkendt af bestyrelsen 23 April 2018

Indholdsfortegnelse

1. Forord og indledning

1.1 Forord

Almindelige og følsomme personoplysninger, samtykkeerklæring, den registerede, databehandleraftaler osv. er blot nogle af de mange nye ord og begreber vi kommer til at høre og arbejde meget mere med i fremtiden.

Grunden til dette, skal findes i den EU Vedtagne persondataforordning, som træder i kraft den 25. maj 2018. Hos Esbjerg International School ønsker vi naturligvis at overholde disse nye love og det omfatter og involvere flere aspekter bl.a. ændrede arbejdsgange og mere anvendelse af it.

Hos Esbjerg International School har vi valgt at lave denne politik, som samler flere politikker i en, dog for at gøre det mere overskueligt og samle vores politik omkring anvendelse af IT og DATA.

Vi ønsker at signalere at vi værner omkring sikkerhed og persondatabeskyttelse både i forhold til bl.a. opbevaring af følsomme personoplysninger, både manuelt og elektronisk. Vi håber med denne politik, at vi fremadrettet får den bedste forståelse ud af denne "nye" verden som vi alle for forpligtet til at opfylde og følge fremadrettet.

Der vil formentlig opstå spørgsmål og tvivl i den kommende tid, så derfor henvend jer gerne til de personer som har med de forskellige ting at gøre og de vil derefter hjælpe jer.

Jesper Hammer
Business Manager

1.2 Indledning

Hver eneste dag anvender vi persondata, det gælder både ansatte og elever.
Det er vigtigt at vi har styr på disse begreber og håndteringen af disse. Hertil anvendes forskellige IT systemer, som på den ene eller anden måde opbevarer og holder styr på de mange forskellige data. IT systemer er nødvendige for at understøtte de mange opgaver som vi står overfor hver dag, dette gælder også anvendelsen af persondata.

Vi er derfor nød til at fastsætte nogle rammer for brugen af IT, herunder hvordan vi behandler data samt sikrer korrekt opbevaring og sletning af data. Det er bl.a. derfor denne politik er blevet udarbejdet, således at vi sikrer os, at vi følger loven og de rammer som skolen har sat sig for

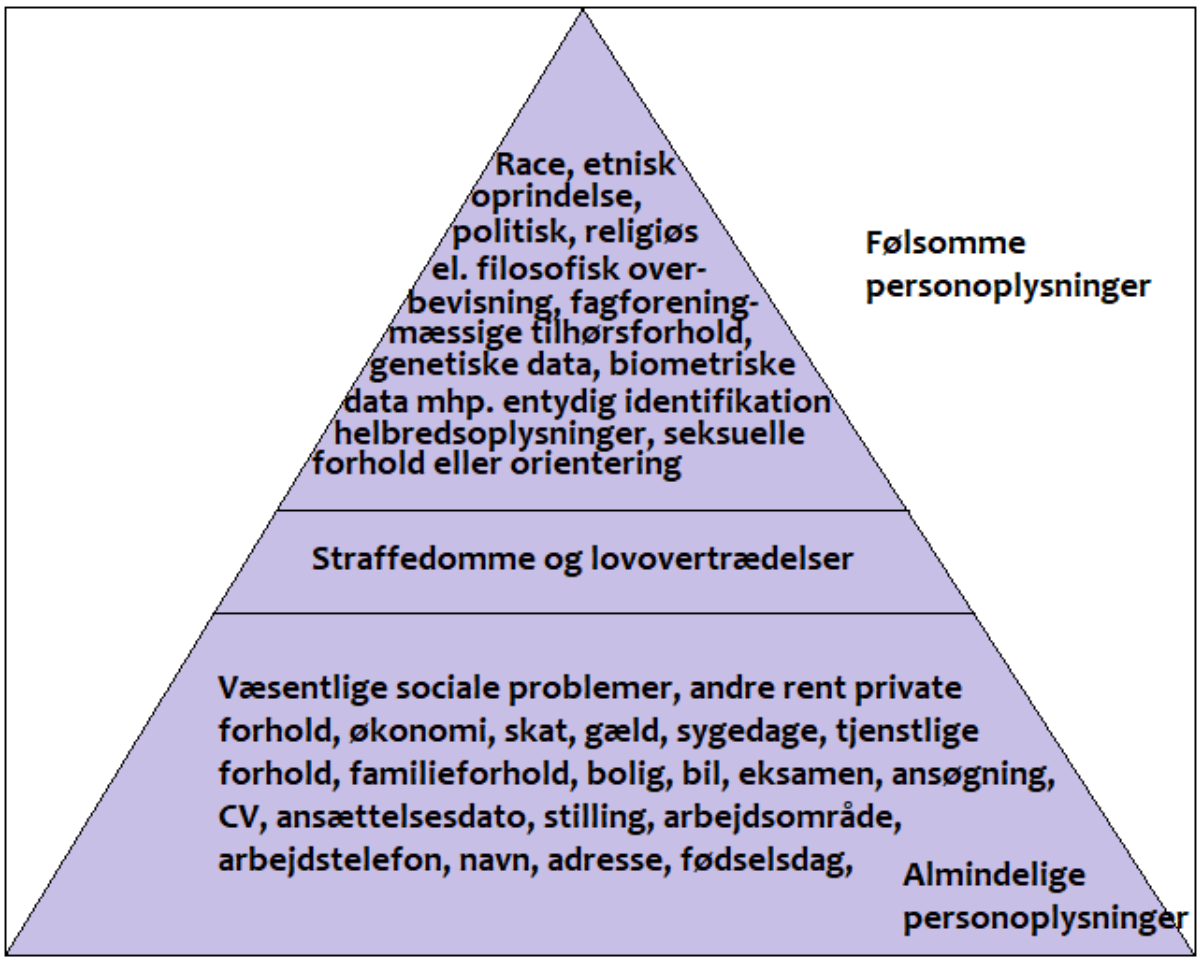
anvendelse af IT og persondata.

EU har skærpet kravene til brugen af IT og specielt til hvordan man håndtere persondata, herunder specielt dokumentationen for brug og anvendelse. Dette har vi forsøgt at tage højde for og indarbejdet i denne politik.

Esbjerg International Schools politikker er opdelt i følgende afsnit:

- Persondatapolitik, som indeholder en beskrivelse af hvordan vi håndtere persondata på Esbjerg International School
- Databeskyttelsespolitik på Esbjerg International School
- Anvendelse af IT til kommunikation på Esbjerg International School med overordnede regler og praksis for, hvordan ansatte og elever skal håndtere kommunikation og anvendelse af IT i dagligdagen

Personoplysninger er enhver form for information om en identificeret eller identificerbar person.



Tegningen herover viser eksempler på, hvad personoplysninger – også kaldet persondata – er, og hvad forskellen er på almindelige personoplysninger og følsomme personoplysninger. Kilde: Datatilsynet

2. Persondatapolitik

2.1 Indledning

Dette afsnit indeholder Esbjerg International Schools politik for håndtering af persondata vedrørende ansatte, elever samt besøg på hjemmesiden.

2.2 Dataansvar / Hvordan behandler vi persondata?

Vi behandler persondata som led i ansættelsen, i forbindelse med elever og ved besøg på skolens hjemmeside.

- Ansatte
  Vi behandler personoplysninger i forbindelse med rekruttering, ansættelse og fratrædelse af medarbejdere. Ansatte har mulighed for at få indsigt i de oplysninger der behandles og i hvilke systemer persondata opbevares. I forbindelse med fratrædelser gælder særlige procedurer for, hvornår persondata slettes

- Elever
  Vi behandler personoplysninger i forbindelse med ansøgning, optagelse, vejledning og undervisning lige indtil en elev får sit skolebevis eller afbryder sin uddannelse.

- Hjemmeside
  Når en bruger besøger vores hjemmeside registrer vi oplysninger om dette til statistikformål. Vi gør altid brugeren opmærksom på dette ved besøg på hjemmesiden. Esbjerg International School opfylder altid gældende love og bekendtgørelser i forbindelse hjemmesidebesøg. For yderligere henvises til skolens cookiepolitik

2.3 Videregivelse af personoplysninger

Som udgangspunkt videregiver Esbjerg International School ikke personoplysninger til 3. part. Der kan dog være lovpligtige regler, der regulere dette. Eksempelvis kan det i forbindelse med skoleskift være nødvendigt at overføre persondata på elever. Der eksisterer særlige procedurer for overførsel af persondata til 3. part. Såfremt der ikke foreligger lovpligtige krav om videregivelse af personoplysninger til 3. part, vil den ansvarlige for behandlingen indhente samtykke fra den person, data omhandler.

2.4 Vi tager databeskyttelse alvorligt

For at beskytte persondata bedst muligt vurderer vi løbende, hvor høj risikoen er for, at vores databehandling påvirker den registreredes grundrettigheder negativt.

I tilfælde af, at de beslutninger, vi har behov for at træffe, er afhængige af, at vi kan behandle følsomme persondata, biometriske oplysninger eller oplysninger om strafbare forhold, gennemfører vi en analyse af konsekvenserne af databehandlingen for sikring af privatlivsbeskyttelse.

2.5 Kontaktoplysninger / Data Protection Officer (DPO)

Esbjerg International School er dataansvarlig og er ansvarlig for at sikre, at persondata behandles i overensstemmelse med lovgivningen.

Skolen har udpeget vores IT ansatte til at sikre, at regler og procedurer i forhold til behandling af personoplysninger overholdes i det daglige.

Spørgsmål til behandlingen af persondata i det daglige på Esbjerg International School kan rettes til:

Haroon Khan (DPO) – IT Manager – E-mail: h.khan@eis.school

Jesper Hammer – Business Manager – E-mail: j.hammer@eis.school

Når vi i politikkerne fx skriver, at "vi beder dig om at stille dine persondata til rådighed for os" vil det typisk være en konkret sagsbehandler, som forestår opgaven efter de fastsatte regler herom.

Skal der sendes fortrolige data til skolen, kan disse sendes til secure@eis.school

2.6 Vi sikrer fair og transparent databehandling

Når vi anmoder om rådighed over persondata, oplyser vi om, hvilke data vi behandler og til hvilket formål. Der udsendes oplysning herom til den berørte på tidspunktet for indsamling af persondata.

Vi giver som hovedregel altid besked om indhentelse af oplysninger hos andre forud for, at det sker. Ellers oplyser vi om det senest 10 dage efter, vi har indhentet persondata. Vi oplyser også om formålet med indhentningen og det lovgrundlag, der giver os adgang til at indhente persondata.

2.7 Vi anvender denne type data

Vi anvender data for at gøre vores service bedre og sikre kvalitet i vores produkter og tjenester samt i vores kontakt med ansatte, elever, forældre og eksterne.

De data vi anvender, omfatter:

2.7.1 Vi behandler kun relevant persondata

Vi behandler kun data, der er relevante og tilstrækkelige i forhold til de formål, der er defineret ovenfor. Formålet er afgørende for, hvilken type data, der er relevante for os. Det samme gælder

omfanget af de persondata, vi bruger. Vi bruger fx ikke flere data, end dem, vi har brug for til det konkrete formål.

Inden vi behandler persondata, undersøger vi, om det er muligt for os at minimere mængden af data. Vi undersøger også om nogle af de datatyper, vi anvender, kan bruges i anonymiseret eller pseudonymiseret form. Det kan vi gøre, hvis det ikke indvirker negativt på vores forpligtelser eller den tjeneste eller service, vi tilbyder.

2.7.2 Vi behandler kun nødvendige persondata

Vi indsamler, behandler og opbevarer kun de persondata, der er nødvendige i forhold til at opfylde vores fastsatte formål. Derudover kan det være bestemt ved lovgivning, hvilken type data der er nødvendig at indsamle og opbevare for vores gennemførelse af uddannelserne. Typen og omfanget af de persondata, vi behandler, kan også være nødvendige for at opfylde en kontrakt eller en anden retlig forpligtelse.

Vi vil gerne være sikre på, at vi kun behandler persondata, der er nødvendige for hvert af vores bestemte formål. Derfor indsamles alene den datamængde, der er nødvendig.

For at beskytte mod, at uvedkommende får adgang til persondata, benytter vi også løsninger, der automatisk sikrer, at data kun er tilgængelige for relevante medarbejdere. Der er også indlejret beskyttelse mod, at et ubegrænset antal personer kan få adgang til data.

2.7.3 Vi kontrollerer og opdaterer persondata

Vi kontrollerer, at de persondata, som vi behandler, ikke er urigtige eller vildledende. Vi sørger også for at opdatere persondata løbende. Da vores service er afhængig af, at data er korrekte og opdaterede, beder vi de registrerede oplyse os om relevante ændringer i data.

For at sikre kvaliteten af data, har vi vedtaget interne regler og fastlagt procedurer for kontrol og opdatering af persondata.

2.7.4 Vi sletter persondata, når de ikke længere er nødvendige

Vi sletter persondata, når de ikke længere er nødvendige i forhold til det formål, som var grunden til indsamling, behandling og opbevaring af data.

2.7.5 Vi indhenter samtykke, inden vi behandler persondata

Vi indhenter samtykke, inden vi behandler persondata til de formål, der er beskrevet ovenfor, med mindre vi har et lovligt grundlag for at indhente dem. Vi oplyser om et sådant grundlag og om vores legitime interesse i at behandle persondata.

Samtykke er frivilligt, og kan til enhver tid trækkes tilbage.

Hvis vi ønsker at anvende persondata til et andet formål end det oprindelige, oplyser vi om det nye formål og beder om samtykke, før vi påbegynder databehandlingen. Hvis vi har et andet lovligt grundlag for den nye behandling, oplyser vi om dette.

Når vi i vores uddannelser og tjenester har behov for at behandle data om unge under 18, år indhenter vi samtykke fra en forælder. Vi kontrollerer så vidt muligt, at samtykket gives af en forælder med forældremyndighed over barnet.

2.7.6 Vi videregiver ikke persondata uden samtykke

Hvis vi videregiver persondata til samarbejdspartnere og aktører, bl.a. til brug for markedsføring, indhenter vi samtykke og informerer om, hvad data vil blive brugt til. Der kan til enhver tid gøres

indsigelse mod denne form for videregivelse. Henvendelser i markedsføringsøjemed kan fravælges i CPR-registret.

Vi indhenter ikke samtykke, hvis vi er retligt forpligtet til at videregive persondata, f.eks. som led i indberetning til en myndighed.

Vi indhenter samtykke, før vi videregiver persondata til samarbejdspartnere i tredjelande. Hvis vi videregiver persondata til samarbejdspartnere i tredjelande, er vi sikre på, at deres niveau for persondatabeskyttelse passer til de krav, vi har opstillet i denne politik efter gældende lovgivning. Vi stiller bl.a. krav til behandlingen af data, til informationssikkerheden og til opfyldelse af de rettigheder, der foreligger i forhold til f.eks. at modsætte sig profilering og indgive klage til Datatilsynet.

2.7.7 Vi beskytter persondata og har interne regler om informationssikkerhed

Vi har vedtaget interne regler om informationssikkerhed, som indeholder instrukser og foranstaltninger, der beskytter persondata mod at blive tilintetgjort, gå tabt eller blive ændret, mod uautoriseret offentliggørelse, og mod, at uvedkommende får adgang eller kendskab til dem.

Vi har fastlagte procedurer for tildeling af adgangsrettigheder til de af vores medarbejdere, der behandler følsomme persondata og data, der afdækker oplysninger om personlige interesser og vaner. Vi kontrollerer deres faktiske adgang gennem logning og tilsyn. For at undgå datatab tager vi løbende backup af vores datasæt. Vi beskytter også fortroligheden og autenciteten af data ved hjælp af kryptering.

I tilfælde af et sikkerhedsbrud, der resulterer i en høj risiko for diskrimination, ID-tyveri, økonomisk tab, tab af omdømme eller anden væsentlig ulempe, vil vi underrette de berørte om sikkerhedsbruddet så hurtigt så muligt.

Hvis man har en formodning om, eller opdager et brud på persondatasikkerheden, skal nærmeste leder straks kontaktes.

2.7.8 Cookies, formål og relevans

Hvis vi placerer cookies, informeres om anvendelsen og formålet med at indsamle data via cookiepolitikken.

Før vi placerer cookies på udstyr, beder vi om samtykke. Nødvendige cookies til sikring af funktionalitet og indstillinger kan dog anvendes uden samtykke. Flere oplysninger om vores brug af cookies, og om hvordan de slettes eller afvises findes på vores hjemmeside. Vejledning om tilbagekaldelse af samtykke findes på vores hjemmeside under cookie-politik.

2.7.9 Ret til at få adgang til egne persondata

Der er til enhver tid ret til at få oplyst, hvilke data vi behandler, hvor de stammer fra, og hvad vi anvender dem til. Det kan endvidere oplyses, hvor længe vi opbevarer persondata, og hvem, der modtager data, i det omfang vi videregiver data i Danmark og i udlandet.

Efter anmodning fra den registrerede, kan vi oplyse om de data, vi behandler. Adgangen kan dog være begrænset af hensyn til andre personers privatlivsbeskyttelse, til forretningshemmeligheder og immaterielle rettigheder.

Ligeledes er der ret til at gøre indsigelse mod vores behandling af persondata.

2.7.10 Ret til at få unøjagtige persondata rettet eller slettet

Hvis den registrerede mener, at de persondata, vi behandler om den pågældende, er unøjagtige, er der ret til at få dem rettet.

I nogle tilfælde vil vi have en forpligtelse til at slette persondata. Det gælder fx, hvis samtykke trækkes tilbage. Finder den registrerede at data ikke længere er nødvendige i forhold til det formål, som vi indhentede dem til, kan der anmodes om sletning af dem. Hvis det formodes, at persondata bliver behandlet i strid med lovgivningen er det vigtigt at gøre opmærksom om dette.

Ved anmodning om at få rettet eller slettet persondata, undersøger vi, om betingelserne er opfyldt, og gennemfører i så fald ændringer eller sletning så hurtigt som muligt.

2.8 Whistleblowerordning på Esbjerg International School

Esbjerg International School har ikke etableret en egentlig whistleblowerordning. Vi har tillid til, at de ansatte anvender og håndterer persondata og it i forhold til den eller de opgaver de er involveret i. Ansatte underskriver en tavshedserklæring og er dermed underlagt tavshedspligt i forhold til de forskellige oplysninger og persondata som de måtte stifte bekendtskab med, som en del af ansættelsen på Esbjerg International School. Får man mistanke om ulovligheder eller uregelmæssigheder omkring persondata eller anvendelsen af it, kontaktes nærmeste leder.

3. Databeskyttelsespolitik

3.1 Indledning

Dette afsnit indeholder skolens politik for beskyttelse af skolens data, herunder de persondata, som vi måtte behandle.

Databeskyttelse er afgørende af flere grunde.

For det første for at sikre, at Esbjerg International Schools følsomme data om elever, kunder, samarbejdspartnere og andre dele af virksomheden ikke kan komme uvedkommende til kendskab.

For det det andet for at sikre, at Esbjerg International School overholder kravene i persondatareglerne for beskyttelse af persondata, herunder følsomme data om medarbejdere og andre personer.

På denne baggrund har Esbjerg International School fastsat en række regler for beskyttelse og håndtering af data i virksomheden.

3.2 Kontaktpersoner

Såfremt der er tvivl om eller spørgsmål til databeskyttelsespolitikken eller om datasikkerhed i øvrigt skal DPO kontaktes – se kontakt info under punkt 2.5

Såfremt der uforvarende er sket overtrædelse af politikken eller opleves andre tilfælde af brud på politikken eller sikkerheden omkring Esbjerg International Schools data skal nærmeste leder kontaktes.

3.3 Anvendelse af IT-systemer og udstyr

Esbjerg International School ønsker at give medarbejdere, elever gode muligheder for brug af it-systemer og udstyr uden unødvendige restriktioner og samtidig sikre mod misbrug af skolens it-systemer og udstyr af andre systemer udført fra skolens installationer.

Vi har tillid til, at medarbejdere og elever udviser ansvarlighed og sund fornuft ved brug af skolens it-systemer og udstyr, og at hver enkelt bruger gør sig bekendt med skolens generelle regler for anvendelse heraf.

Alle anskaffelser af digitalt udstyr i form af pc, tablet, mobiltelefon og software skal ske gennem it-afdelingen via nærmeste leder.

Der kan forekomme lokale anvendelsespolitikker med skærpede krav.

Brug af it-faciliteterne:

- Undervisnings- og arbejdsrelateret anvendelse af skolens it-systemer og udstyr har altid fortrinsret frem for privat anvendelse
- Skolens it-systemer og udstyr kan benyttes til private formål under hensyn til nærværende politikker
- It-administratorer skal sikre, at it-systemer og udstyr ikke anvendes i strid med formålet. Det betyder, at it-administratorer kan gennemse email og andre dokumenter. Al "trafik" logges. Materiale gemmes.
- For at undgå misbrug skal brugeren logge af eller slukke, når brugeren forlader udstyret
- Netværkets brugere har pligt til at holde egen adgangskode hemmelig. Har en bruger mistanke om, at andre kender ens egen kode, skal brugeren omgående ændre dem
- Udvis netetik. Det betyder bl.a. at brugeren behandler andre brugere på nettet med respekt. Sørg f.eks. for at egne indlæg altid kan "tåle" at blive set af udenforstående
- Undgå unødig udskrivning. Vær ressourcebevidst.
- Når der behandles oplysninger elektronisk, benyttes kun sikre og godkendte it-systemer
- Anvendelse af privat pc, tablet og mobiltelefon til arbejdsbrug skal ske i overensstemmelse med indgået "tro og lovererklæring"
- Hvis man støder på materiale og adfærd, som er i strid med nærværende politikker kontaktes nærmeste leder.

Eksempler på uacceptabel brug af it-faciliteterne:

- It-udstyret må ikke bruges til obskøn aktivitet eller aktivitet, der er forbudt ifølge dansk lovgivning, herunder love og regler om ophavsret.
- Brugeren må ikke ændre maskinens opsætning eller udseende, uden at det er aftalt med den it-ansvarlige
- Det er ikke tilladt at bruge it-systemerne og udstyret til kommercielle formål, privat markedsføring, politisk agitation eller offentliggørelse af private oplysninger om en anden person.
- Brugerne må ikke logge på med en anden persons identitet eller forsøge at få adgang til andre brugers eller organisationens filer (hacking). Brugeren må ikke skjule sin identitet, bortset fra de tilfælde hvor det eksplicit er tillagt.
- Brugerne må ikke deltage i kædebreve eller sende uhensigtsmæssigt mange e-mail af sted på én gang (spam)

- Det er ikke lovligt at installere skolens programmer på privat pc, tablet og telefon uden it-afdelingens godkendelse.
- Der må som hovedregel ikke gemmes oplysninger med følsomt indhold om andre.

Konsekvenser ved uacceptabel brug af it-faciliteterne:

- Adfærd i strid med it-anvendelsespolitikken medfører sanktioner og i grove tilfælde politianmeldelse
- Sanktioner kan være såvel mundtlig eller skriftlig advarsel som bortvisning.

På Esbjerg International School anvender vi kun it-systemer som er godkendte og installerede af it-afdelingen. Al indkøb og installation af it-systemer foretages som udgangspunkt af it-afdelingen. Der kan være enkeltstående eller særlige forhold som gør, at andre end it-afdelingen installerer it-systemer, f.eks. anvendelse af systemer som driftes af andre.

For yderligere omkring indkøb, installation og anvendelse af it-systemer og udstyr henvises til it-afdelingen.

For at kunne udføre support på en effektiv måde, definerer it-afdelingen standarder for anskaffelser, installation/opdatering, indfasning/fornyelse, bortskaffelse af udstyr samt opsætning af pc arbejdspladser og undervisningslokaler, printere mm.

3.4 Databehandleraftaler

I forbindelse med persondataforordningen er det vedtaget, at skolen skal indgå aftaler med de it-leverandører, der behandler personoplysninger på skolens vegne. Til brug herfor anvender skolen en standardskabelon udarbejdet til formålet. Der indhentes skriftlig aftale med de it-leverandører, som skolen anvender til behandling af personoplysninger.

De indgåede aftaler journaliseres og arkiveres i skolens arkivsystem. Yderligere oplysninger kan fås ved henvendelse til it-afdelingen.

Det er kun it-afdelingen, der indhenter og godkender databehandleraftaler.

3.5 E-mails- og internetbrug (sociale medier mv)

Al kommunikation, herunder e-mails på skolens netværk anses for skolens ejendom og skal ske i overensstemmelse med skolens retningslinjer.

E-mails og anden kommunikation og internetbrug på skolens udstyr og ejendom, som angår privatsfæren, må kun ske undtagelsesvist og skal overholde gældende regler om it-sikkerhed, adfærd og brug af skolens ejendom.

Brug af skolens it-udstyr og ejendom må ikke have pornografisk, politisk ekstremistisk eller diskriminerende karakter for så vidt angår alder, handicap, race, køn, etnisk eller social oprindelse eller religion.

Ved fratræden – og i tilfælde af fritstilling – skal alle referencer til nutidig ansættelse eller tilknytning i virksomheden slettes på sociale medier, som medarbejderen kontrollerer og/eller kan ændre i.

Filer, der tilhører tredjemand, må ikke downloades i strid med rettigheder eller på anden måde kopieres eller overføres til skolens udstyr og ejendom. Sådanne filer er eksempelvis, men ikke

begrænset til, filmklip, billeder, spil, softwareprogrammer og lign. Tilsvarende må der ikke ved brug af e-mail sendes materiale i strid med rettighedsreglerne.

E-mails fra personer eller virksomheder eller organisationer, der ikke er kendte og spam-mails bør altid håndteres med stor forsigtighed og ved tvivl bør itafdelingen kontaktes.

E-mails, filer eller links fra ukendte kilder bør aldrig åbnes eller klikkes på. Tilsvarende gælder e-mails, filer eller links sendt fra kendte kilder, hvis der er nogen grund til tvivl om autenticiteten eller sikkerheden ved det fremsendte.

I det omfang der undtagelsesvist kan være behov for at anvende eller håndtere e-mails eller internettet i strid med ovennævnte kræver det godkendelse fra it-afdelingen

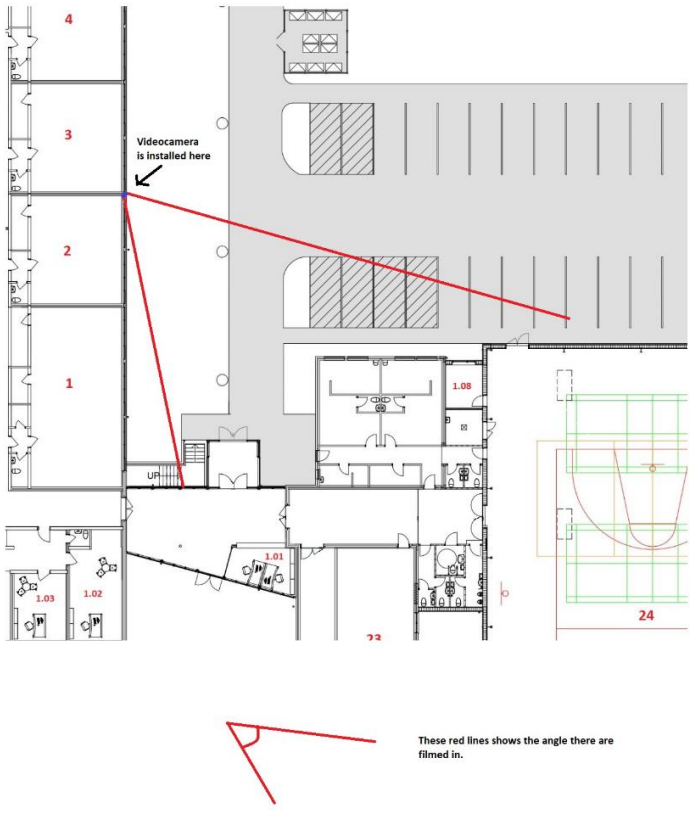
3.6 Passwords

I forhold til håndtering af passwords er det vigtigt at være opmærksom på, at:

- Passwords skal altid opbevares hemmeligt og sikkert.
- Passwords må ikke oplyses eller videregives til andre.
- Passwords skal altid ændres med jævne mellemrum, dog minimum en gang årligt. Password skal, hvor det er muligt, være på minimum 8 tegn bestående af tal, bogstaver og tegn.
- Nedskrevne passwords må ikke opbevares ved pc'en.

3.7 Videoovervågning

EIS har februar 2021 indført videoovervågning af hovedindgangen og noget af parkeringspladsen. Dette er gjort for at øge sikkerheden samt sikre bedre forsikringsforhold.
Videomaterialet bliver opbevaret på skolens interne server i 7 dage, hvorefter det slettes.
Det er kun skolens IT Manager der har adgang videomaterialet. Der forefindes ligeledes et afsnit herom i skolens håndbog til ansatte. Her ses en tegning af overvågningens placering:



3.8 Manuel opbevaring af personfølsomdata

Esbjerg International School opbevarer en vis mængde manuel/fysisk mængde papirer med personfølsomme data på. Et eksempel på dette kunne være en ansættelseskontrakt, lønseddel eller en indmeldelsesblanket. Disse opbevares forsvarligt og står låst inde i skabe til dagligt på kontorer som er aflåste når personerne som har adgang til disse oplysninger, ikke er på kontoret.

3.9 Bortskaffelse af personfølsomme data

Esbjerg International School bortskaffer personfølsomme data efter de givne regler. Dette vedr. bl.a. ansøgninger, gamle ansættelseskontrakter, elev-blad osv. Disse slettes fra vores systemer når vedkommende ikke længere er ansat eller går på skolen. Fysiske papirer bliver makuleret i en aflåst spand.

4.0 Sanktioner

Manglende overholdelse af databeskyttelsespolitikken kan afhængig af forholdets grovhed eventuelt medføre tjenestelig påtale, medføre advarsel, opsigelse eller bortvisning.