

# Vejledning til håndtering af fund af børnepornografisk materiale på arbejdspladsen

Udgivet af: Red Barnet og DI ITEK  
Redaktion: Kuno Sørensen og Henning Mortensen  
ISBN: 978-87-7353-938-5  
0.11.11

## **Indledning**

Denne vejledning er lavet for at ruste danske virksomheder til at tage en drøftelse af, hvordan de vil forholde sig, hvis der skulle findes "utugtige billeder af børn", i daglig tale kaldet "børnepornografi" eller "billeder af seksuel udnyttelse af børn" på arbejdspladsens computere, elektroniske apparater, bærbare medier og / eller netværk.

Vejledningen lister juridiske fakta på området, giver en tjekliste over nogle af de forhold virksomheden bør forholde sig til og giver desuden et forslag til en retningslinje til uddybning af informationssikkerhedspolitikken. Det anbefales, at disse ting diskuteres og fastlægges inden et evt. fund finder sted.

I vejledningen anvendes begrebet "billeder af seksuel udnyttelse af børn" i stedet for ordet "børneporno".

## **Kend loven**

Den relevante lovgivning er indeholdt i straffelovens § 230 og § 235<sup>1</sup>.

Det er vigtigt, at virksomheden forstår lovgivningen om "utugtige billeder af børn", som billeder og film af seksuel udnyttelse af børn hedder i straffeloven. Specifikt:

- Det er strafbart at besidde, distribuere, vise og producere utugtige billeder af børn.
- Det er også strafbart at se utugtige billeder af børn på internettet, også selv om billederne ikke bliver downloadet.
- Straffeloven definerer i denne sammenhæng "børn" som alle personer under 18 år.

Som en ansvarlig virksomhed bør det sikres, at virksomhedens ledelse og medarbejdere er klædt på til at håndtere, at der på virksomhedens udstyr kan findes ulovlige eller krænkende billeder af børn som defineret i lovgivningen.

## **Ledelsesbeslutning**

Det er ledelsens opgave at beslutte, hvilken indsats virksomheden skal gøre på dette område. Først og fremmest bør virksomhedens ledelse drøfte fordele og ulemper ved at have en retningslinje for bekæmpelse af billeder af seksuel udnyttelse af børn på arbejdspladsen. Virksomhederne kan bidrage til bekæmpelse af kriminalitet. Desuden kan der være både sikkerhedsmæssige fordele og CSR-fordele<sup>2</sup> ved at have en sådan retningslinje.

---

<sup>1</sup> Straffelovens relevante paragraffer kan findes her:

<https://www.retsinformation.dk/Forms/R0710.aspx?id=133530#K24>.

<sup>2</sup> Corporate Social Responsibility

Retningslinjen bør først og fremmest adressere, hvordan man håndterer tilfælde med billeder af seksuel udnyttelse af børn - herunder:

- Gør det klart for alle medarbejdere i virksomheden, hvad de skal gøre, hvis et billede af seksuel udnyttelse af et barn opdages, og hvem i virksomheden der tager hånd om problemet.
- Udpege et kontaktpunkt - f.eks. nærmeste chef tillige med en medarbejder i HR - som kan kontaktes ved en oplevelse af billeder af seksuel udnyttelse af børn.
- Klart beskrive en retningslinje for, hvordan medarbejdere i kontaktpunktet håndterer situationer, hvor medarbejdere på arbejdspladsen har oplevet eller er afsløret i at være i besiddelse af billeder af seksuel udnyttelse af børn.
- Sørge for at kontaktpunktet på den ene side har adgang til de ressourcer de har behov for, og på den anden side sørger for at så få mennesker som muligt involveres i processen bag opklaringen.
- Besiddelse, visning m.m. af utugtige billeder af børn er forbudt ifølge dansk lovgivning. Der skal derfor tages stilling til om anmeldelse - til Red Barnet, politiet eller andre - skal finde sted. DI og Red Barnet anbefaler, at anmeldelse altid finder sted.
- Tydeliggøre de ansættelsesmæssige konsekvenser ved besiddelse af billeder af seksuel udnyttelse af børn.
- Tager stilling til om og i givet fald i hvilket omfang virksomheden vil installere tekniske foranstaltninger til at opdage, behandle og blokere billeder af seksuel udnyttelse af børn.

## **Information til personalet**

For at virksomhedens politikker og retningslinjer skal være effektive, skal de være let tilgængelige, og hver medarbejder skal kende og forstå indholdet. Nogle virksomheder forvalter dette ved, at den enkelte medarbejder får tilsendt en kopi af politikker og retningslinjer og kvitterer for modtagelsen. Andre virksomheder sikrer, at politikker og retningslinjer altid er tilgængelige - f.eks. via intranet. Ved nye tiltag er det vigtigt, at der afholdes informationsmøder eller på anden måde tydeligt gøres opmærksom på tiltagene.

Virksomhedens Samarbejdsudvalg eller tillidsrepræsentanter bør forelægges retningslinjerne forud for information til medarbejderne. Man kan give en seks ugers frist til ikrafttrædelse af retningslinjen.

Virksomheden skal desuden være opmærksom på, at når der behandles personfølsomme oplysninger i personaleadministrationen skal der være foretaget en anmeldelse til Datatilsynet. Dette gælder helt generelt og er ikke betinget af tiltag rettet mod bekæmpelse af billeder af seksuel udnyttelse af børn.

## Yderligere information og mulige tiltag

Som nævnt ovenfor er den første og vigtigste opgave, at ledelsen forholder sig til billeder af seksuel udnyttelse af børn og laver en retningslinje. Der er en række ekstra tiltag, som det er muligt at tage. Desuden er der en række steder, hvor man kan få ekstra hjælp til at bekæmpe billeder af seksuel udnyttelse af børn:

Tekniske foranstaltninger:

- Vær omfattet af den danske blokeringsordning. De danske netudbydere samarbejder med Rigspolitiet og Red Barnet om at blokere for adgangen til udenlandske hjemmesider, der indeholder billeder af seksuel udnyttelse af børn. Du kan undersøge, om din netforbindelse er omfattet af ordningen hos politiet, <http://www.politi.dk/da/borgerservice/boernepornofilter/filter01102007.htm>:
- Installer software, som kan identificere ulovlige billeder af seksuel udnyttelse af børn. Red Barnet har konkrete anbefalinger til hvilket software, der kan anvendes. Se mere på [www.redbarnet.dk](http://www.redbarnet.dk).
- Anti-spam software vil hjælpe med at begrænse e-mails, som reklamerer for potentielt kriminelle billeder, idet disse e-mails ofte vil blive udsendt som spam.
- Firewalls vil hjælpe med at forhindre uautoriseret adgang til arbejdspladsens computer-systemer og forhindre nogen i at bruge dem til at gemme potentielt kriminelle billeder.

Hjælp fra professionelle organisationer:

- Informer om hjælpemuligheder. Voksne, der interesserer sig for seksuelle billeder af børn, mangler ofte hjælp eller redskaber til at stoppe deres lyster og fantasier. Udbred kendskabet til hjemmesiden [www.brydcirklen.dk](http://www.brydcirklen.dk) som henvender sig med hjælp og rådgivning til voksne, der seksuelt interesserer sig for børn.
- Red Barnet er en organisation, der arbejder med at beskytte børns rettigheder. Red Barnet har stor erfaring i at bekæmpe billeder af seksuel udnyttelse af børn og stiller gerne op med gode praktiske råd - også til virksomhederne. Red Barnet har desuden en hotline, hvor man kan anmelde hjemmesider med billeder af seksuel udnyttelse af børn. Se mere på [www.redbarnet.dk](http://www.redbarnet.dk).
- Anmeldelse af billeder af seksuel udnyttelse af børn på hjemmesider og lignende kan ske til Red Barnet [www.redbarnet.dk/anmeld](http://www.redbarnet.dk/anmeld), til dit lokale politi eller til Rigspolitiets Nationale IT-efterforskningscenter, NITEC, [www.politi.dk/da/hjaelppolitiet/itkriminalitet/](http://www.politi.dk/da/hjaelppolitiet/itkriminalitet/).

## **Skabelon til retningslinje**

Nedenfor findes en skabelon til retningslinje for bekæmpelse af billeder af seksuel udnyttelse af børn på arbejdspladsen. Virksomhedens ledelse bør tilpasse skabelonen, så den passer til virksomhedens værdier og er i overensstemmelse med lokalt tilpassede og fastlagte regler.

I retningslinjen er omtalt HR-chef, AH-afdeling, IT-chef, IT-ansvarlig og Personalejura. For mindre virksomheder skal disse begreber opfattes som den person, der har ansvaret for de pågældende områder.

## **Retningslinje**

Produktion, distribution, fremvisning og besiddelse af utugtige billeder af børn er strafbart i henhold til straffelovens § 230 og § 235. Virksomhedens ledelse finder, at enhver oplevelse af billeder af seksuel udnyttelse af børn hos medarbejderne er uacceptabel, og disse oplevelser skal håndteres i overensstemmelse med nærværende retningslinje.

Virksomheden vil med denne retningslinje tydeliggøre, hvordan medarbejderne skal forholde sig til billeder af seksuel udnyttelse af børn og desuden indskærpe hvilke konsekvenser - ansættelsesretligt såvel som strafferetligt - besiddelse af billeder af seksuel udnyttelse af børn vil have for den enkelte medarbejder.

Retningslinjen finder sted på alt udstyr, som ejes af virksomheden, tillige med alt udstyr, som tilsluttes virksomhedens infrastruktur.

Virksomheden har tavshedspligt i forhold til følsomme personoplysninger om en berørt medarbejder. Virksomheden tilstræber, at behandling af sager inddrager så få medarbejdere i virksomheden som muligt.

## **Kontaktpunkt**

Hvis en medarbejder oplever billeder af seksuel udnyttelse af børn i forbindelse med sit arbejde - f.eks. uagtet kommer ind på en hjemmeside der indeholder billeder af seksuel udnyttelse af børn, finder billeder af seksuel udnyttelse af børn på et fællesdrev eller opdager billeder af seksuel udnyttelse af børn hos en kollega - skal medarbejderen tage kontakt til nærmeste chef.

Enhver chef, der selv oplever eller fra en medarbejder bliver gjort opmærksom på billeder af seksuel udnyttelse af børn, skal rette henvendelse til et kontaktpunkt i HR, e-mail: yyy, tlf.: zzz.

HR vil iværksætte de rutiner, der er beskrevet nedenfor. I det omfang HR skønner det nødvendigt, vil HR inddrage kompetencer fra IT eller fra Personalejura.

## Mulige scenarier

### ***Hvad skal en ansat gøre, hvis den ansatte uforvarende bliver udsat for billeder af seksuel udnyttelse af børn, mens de bruger internettet?***

- Medarbejderen kontakter nærmeste chef.
- Nærmeste chef kontakter HR.
- De webadresser (hjemmeside-adresser), som indeholder ulovlige eller mistænkelige billeder skal indberettes til Red Barnets Internet Hotline på [www.redbarnet.dk](http://www.redbarnet.dk). Indberetningen foretages af en udpeget medarbejder fra HR.
- Der fremsendes til Red Barnet alene webadresser og ikke kopier af de pågældende billeder.
- Virksomheden blokerer de pågældende sider i sin firewall eller sikrer gennem andre tekniske løsninger (f.eks. abonnement på filter), at siderne blokeres.
- Der er ingen strafferetlige eller ansættelsesretlige konsekvenser.

### ***Hvad skal en ansat gøre, hvis den ansatte finder billeder af seksuel udnyttelse af børn på fælles ressourcer på virksomhedens elektroniske enheder?***

- Medarbejderen kontakter nærmeste chef.
- Nærmeste chef kontakter HR.
- HR kontakter IT for at finde ud af, hvordan indholdet er havnet på den fælles ressource og for at bevissikre materialet. Det vurderes, i hvilket omfang der skal søges efter yderligere potentielt kriminelt materiale på virksomhedens udstyr.
- Hvis HR er i tvivl om, hvorvidt billederne er kriminelle, kontaktes politiet med henblik på at afgøre, om billederne er kriminelle eller ej. HR kan vælge at kontakte det lokale politi eller også gå ind via [www.politi.dk/da/hjaelppolitiet/itkriminalitet/](http://www.politi.dk/da/hjaelppolitiet/itkriminalitet/) og anmelde forholdet til Rigspolitiets it-efterforskningscenter, NITEC. På [www.politi.dk](http://www.politi.dk) er der kontaktoplysninger for den lokale politikreds.
- Det pågældende materiale krypteres og indberettes til politiet jævnt ovenstående.
- Indberetningen foretages af en udpeget medarbejder fra HR.
- Hvis IT finder ud af, at der er tale om sikkerhedsbrud, lukkes hullet til den pågældende ressource. Der er i denne situation ingen strafferetlige eller ansættelsesretlige konsekvenser.
- Hvis IT finder ud af at indholdet er placeret på lokationen af en medarbejder (eller ekstern konsulent) inddrages Personalejura.
- HR, IT og Personalejura skaber sig overblik over omfanget af materialet. Personalejura orienterer medarbejderens chef. Der foretages en vurdering af, om materialets omfang kræver politianmeldelse. Herunder om der kræves politianmeldelse, inden medarbejderen orienteres (med henblik på evt. ransagelse hos medarbejderen).
- Virksomheden foretager som udgangspunkt anmeldelse til politiet og suspension af medarbejderen.

- Der foretages en opklarende samtale med medarbejder (eller ekstern konsulent), Personalejura og chef. Hvis der er foretaget politianmeldelse, bør man afvente at politiet giver grønt lys for samtalen.
- Ved samtalen vurderes medarbejderens (eller den eksterne konsulents) reaktion, forklaring, bevidst/ubevidst kigget på porno, bevidst/ubevidst brugt virksomhedens it udstyr til formålet, tilsluttet privat udstyr til arbejds-pc og beredvillighed til / nægtelse af at bidrage til opklaring.
- På baggrund af samtalen og materialets omfang vurderes konsekvenser for medarbejderen - herunder bortvisning.
- Hvis der er tale om en ekstern konsulent, vurderes samarbejdsaftalen med det pågældende firma.
- Hvis nogle kopier skal opbevares på anmodning af politiet, så bør de opbevares sikkert, hvor ingen andre har adgang til dem. Det vurderes, om materialet tillige skal slettes fra eventuel backup.
- Alle andre kopier skal slettes.
- Håndteringen af sagens forløb vurderes af HR, Personalejura og IT og retningslinjen kan evt. tilpasses, hvis der er opstået uhensigtsmæssigheder.

***Hvad skal en ansat gøre, hvis den ansatte opdager billeder af seksuel udnyttelse af børn hos en kollega?***

- Medarbejderen kontakter nærmeste chef.
- Nærmeste chef kontakter HR.
- HR kontakter IT for at materialet kan bevissikres. Det vurderes i hvilket omfang der skal søges efter yderligere potentielt kriminelt materiale på virksomhedens udstyr.
- Hvis HR er i tvivl om, hvorvidt billederne er kriminelle, kontaktes politiet med henblik på at afgøre, om billederne er kriminelle eller ej. HR kan vælge at kontakte det lokale politi eller også gå ind via [www.politi.dk/da/hjaelppolitiet/itkriminalitet/](http://www.politi.dk/da/hjaelppolitiet/itkriminalitet/) og anmelde forholdet til Rigspolitiets it-efterforskningscenter, NITEC. På [www.politi.dk](http://www.politi.dk) er der kontaktoplysninger for den lokale politikreds.
- Det pågældende materiale krypteres og indberettes til politiet jævnfør ovenstående.
- Indberetningen foretages af en udpeget medarbejder fra HR.
- HR inddrager Personalejura.
- HR, IT og Personalejura skaber sig overblik over omfanget af materialet. Personalejura orienterer medarbejderens chef. Der foretages en vurdering af, om materialets omfang kræver politianmeldelse. Herunder om der kræves politianmeldelse inden medarbejderen orienteres (med henblik på evt. ransagelse hos medarbejderen).
- Virksomheden foretager som udgangspunkt anmeldelse til politiet og suspension af medarbejderen.
- Der foretages en opklarende samtale med medarbejder (eller ekstern konsulent), Personalejura og chef. Hvis der er foretaget politianmeldelse, bør man afvente at politiet giver grønt lys for samtalen.
- Ved samtalen vurderes medarbejderens reaktion, forklaring, bevidst/ubevidst kigget på porno, bevidst/ubevidst brugt virksomhedens it udstyr til formålet, tilsluttet privat udstyr til arbejds-pc og beredvillighed til / nægtelse af at bidrage til opklaring.

- På baggrund af samtalen og materialets omfang vurderes konsekvenser for medarbejderen - herunder bortvisning.
- Hvis nogle kopier skal opbevares på anmodning af politiet, så bør de opbevares sikkert, hvor ingen andre har adgang til dem. Det vurderes, om materialet tillige skal slettes fra eventuel backup.
- Alle andre kopier skal slettes.
- Håndteringen af sagens forløb vurderes af HR, Personalejura og IT og retningslinjen kan evt. tilpasses, hvis der er opstået u hensigtsmæssigheder.

***Hvad skal en IT-medarbejder gøre, hvis medarbejderen fra IT-afdelingen opdager billeder af seksuel udnyttelse af børn hos en medarbejder eller ekstern konsulent?***

- Medarbejderen kontakter IT-chefen.
- IT-chefen kontakter HR.
- IT-afdelingen bevissikrer materialet. Det vurderes, i hvilket omfang der skal søges efter yderligere potentielt kriminelt materiale på virksomhedens udstyr.
- Hvis HR er i tvivl om, hvorvidt billederne er kriminelle, kontaktes politiet med henblik på at afgøre, om billederne er kriminelle eller ej. HR kan vælge at kontakte det lokale politi eller også gå ind via [www.politi.dk/da/hjaelppolitiet/itkriminalitet/](http://www.politi.dk/da/hjaelppolitiet/itkriminalitet/) og anmelde forholdet til Rigspolitiets it-efterforskningscenter, NITEC. På [www.politi.dk](http://www.politi.dk) er der kontaktoplysninger for den lokale politikreds.
- Det pågældende materiale krypteres og indberettes til politiet jævnfør ovenstående.
- Indberetningen foretages af en udpeget medarbejder fra HR.
- HR inddrager Personalejura.
- HR, IT og Personalejura skaber sig overblik over omfanget af materialet. Personalejura orienterer medarbejderens chef. Der foretages en vurdering af, om materialets omfang kræver politianmeldelse. Herunder om der kræves politianmeldelse inden medarbejderen orienteres (med henblik på evt. ransagelse hos medarbejderen).
- Virksomheden foretager som udgangspunkt anmeldelse til politiet og suspension af medarbejderen.
- Der foretages en opklarende samtale med medarbejder (eller ekstern konsulent), Personalejura og chef. Hvis der er foretaget politianmeldelse, bør man afvente at politiet giver grønt lys for samtalen.
- Ved samtalen vurderes medarbejderens (eller den eksterne konsulents) reaktion, forklaring, bevidst/ubevidst kigget på porno, bevidst/ubevidst brugt virksomhedens it udstyr til formålet, tilsluttet privat udstyr til arbejds-pc og beredvillighed til / nægtelse af at bidrage til opklaring.
- På baggrund af samtalen og materialets omfang vurderes konsekvenser for medarbejderen (eller ekstern konsulent) - herunder bortvisning.
- Hvis der er tale om en ekstern konsulent, vurderes samarbejdsaftalen med det pågældende firma.
- Hvis nogle kopier skal opbevares på anmodning af politiet, så bør de opbevares sikkert, hvor ingen andre har adgang til dem. Det vurderes, om materialet tillige skal slettes fra eventuel backup.
- Alle andre kopier skal slettes.
- Håndteringen af sagens forløb vurderes af HR, Personalejura og IT og retningslinjen kan evt. tilpasses, hvis der er opstået u hensigtsmæssigheder.