Utdannings-
direktoratet

Hvordan beskytte barn mot skadelig innhold på nett?

Hva skal barnehager og skoler gjøre for å hindre at barn og elever får tilgang til skadelig innhold på nett?

VEILEDNING | SIST ENDRET: 21.11.2019

Innhold

Hva er alvorlig skadelig innhold?

Tilgang til internett i barnehage og skole oppfattes ofte som en risiko fordi barn kan få tilgang til innhold som ikke er beregnet for dem. Enten barna har søkt aktivt selv eller kommet over skadelig innhold på nett ved et uhell, er det barnehage- og skoleeieres ansvar å forebygge det.

Barnehage- og skoleeiere må ha rutiner for å forebygge, skjerme og håndtere tilgang til alvorlig skadelig innhold. Dette kan være filmer, videoklipp, tekst, illustrasjoner, bilder, spill, lyd og animasjoner.

> I Bildeprogramloven defineres alvorlig skadelig innhold som «Skildringer i bildeprogram som kan virke sterkt følelsesmessig opprivende eller sterkt kognitivt forstyrrende for mindreåriges velbefinnende, særlig nærgående skildringer av kjønnslig aktivitet, grov vold og annen svært forstyrrende eller skremmende tematikk.»

Eksempler på skadelig innhold kan også være diskusjoner og illustrasjoner om selvskading, innhold eller måter for å bli/være veldig tynn, erfaringer med narkotika, eller metoder for å begå selvmord.

Barnehage- og skoleeieres ansvar

Barnehage- og skoleeiere har et ansvar for å ivareta barnas sikkerhet og personvern når de tar i bruk digitale enheter. Det forutsetter både tekniske løsninger tilpasset den enkelte barnehage- og skoleeiers behov og kompetanse hos barn, ansatte og ledelse. Det forutsetter også organisatoriske grep, rutiner, retningslinjer og opplæring knyttet til bruk av digitale enheter i undervisning og administrasjon.

De aller fleste barnehage- og skoleeiere er bevisst på sitt ansvar når de deler ut nettbrett og annet utstyr til barn og ansatte. Tekniske løsninger alene er ikke tilstrekkelig for å sikre barna trygge og gode digitale læringsmiljø. Barnehage- og skoleeiere må kontinuerlig vurdere hvilke tekniske muligheter som er tilgjengelig og finne gode løsninger for å realisere dem på en måte som er tilpasset deres behov.

Rettslige rammer

Barnehage- og skoleeiere må være bevisst på bestemmelsene i barnekonvensjonen, barnehageloven og opplæringsloven. Reglene i personvernloven er også viktig.

Barn har rett til ytringsfrihet, som omfatter frihet til å søke, motta og spre informasjon og ideer av alle slag og på alle måter. Dette er også omtalt i Barnekonvensjonen.

Barnehageeier har ansvar for at reglene i barnehageloven med forskrifter følges. Se rammeplan for barnehage om digital praksis.

Digitale ferdigheter er en av de grunnleggende ferdighetene i skolen. Digitale ferdigheter vil si å innhente og behandle informasjon, være kreativ og skapende med digitale ressurser, og å kommunisere og samhandle med andre i digitale omgivelser. Det innebærer å kunne bruke digitale ressurser hensiktsmessig og forsvarlig for å løse praktiske oppgaver.

Hvordan jobbe forebyggende?

Teknologien kan hjelpe med å fjerne uønsket innhold, men barnehagen og skolen må fortsatt ha fokus på nettvett hos barna, slik at de blir rustet til å håndtere situasjoner hvor de får treff på skadelig innhold. Det er

viktig å ha et samarbeid med foreldrene, slik at de også kjenner til dette.

Digital dømmekraft

Digital dømmekraft innebærer å kunne bruke digitale verktøy, medier og ressurser på en forsvarlig måte, og å ha et bevisst forhold til personvern og etisk bruk av internett. Akkurat som man ikke lærer seg å skrive eller lese på en dag, må digitale ferdigheter utvikles over tid, noe skolen har ansvar for.

Å utvikle digital dømmekraft betyr at barn og unge tilegner seg kompetanse som kan forebygge uønskede hendelser på nett. Denne kompetansen må barnehager og skoler bidra til å utvikle. Det er barnehage- og skoleeier som må sørge for at de ansatte i barnehager og skoler har den nødvendige kompetansen.

Hensiktsmessig bruk av IKT og digital dømmekraft bør også settes på agendaen i samarbeidet mellom barnehage/skole og foreldre, for eksempel som tema på foreldremøter.

Barn som utvikler digital kompetanse har større sannsynlighet for å mestre risiko på nett og utvikle strategier for å håndtere potensielt skadelige situasjoner. Barnehagen og skolen har derfor en viktig rolle i å utjevne ulikheter i barns digitale kompetanse og sørge for at alle barn har like muligheter til å få positive opplevelser på nett.

Hvordan forebygge at barn aktivt søker opp skadelig innhold?

- Involver elevene i arbeidet med å utvikle IKT-reglement, og snakk om hva som er hensikten med reglementet.
- Jobb med tydelig klasseledelse og skap gode relasjoner med barna.

Hvordan forebygge utilsiktet tilgang til skadelig innhold?

- Enheter som kan kobles til nett bør brukes under oppsyn av voksne
- Bruk av «begrenset tilgang»-løsninger og tekniske skjermingsløsninger

Voksne trenger også økt kompetanse

Barn og unge trenger å vite hva de skal gjøre dersom de opplever noe ubehagelig på nett. Voksne må vite hvordan de skal reagere og håndtere situasjonene, slik at de kan hjelpe barna, blant annet hvordan med hvordan de skal bearbeide skremmende opplevelser.

I et helhetlig arbeid med barnehage- og skolemiljø er det viktig å inkludere barns digitale opplevelser. Ved å utvikle gode strategier for hensiktsmessig bruk av digitale enheter, vil barn og voksne være bedre forberedt til å håndtere negative opplevelser knyttet til nettbruk.

En av de store utfordringene i dag, er at barn og unge ikke ber om hjelp og veiledning fra voksne dersom de opplever noe ubehagelig eller skremmende på nett. Kompetanseheving av personell er derfor et viktig forebyggende tiltak. For å kunne sette seg inn i barns opplevelser på nett, trenger voksne i barns nærhet

kunnskap og kompetanse om barns liv på nett og hvilke erfaringer de gjør seg der. Voksne må tilrettelegge for barns utvikling.

Viktig å tenke på:

- Betydningen av å jobbe med digitale retningslinjer eller IKT-reglement
- Effekten av å jobbe med tydelig voksen-/klasseledelse og gode relasjoner med barna
- Konsekvent håndheving av retningslinjer
- Betydningen av et godt barnehage-hjem- og skole-hjem-samarbeid

Tekniske løsninger for skjerming

Begrenset innhold-modus er et alternativ for skjerming av barn for skadelig innhold. Begrenset innhold-modus kan brukes i søkemotorer eller tjenesteplattformer som sosiale media, underholdningsportaler, søkemotorer dedikert til barn, bloggtjenester eller andre.

På noen av plattformene er det relativt enkelt å eliminere innhold som ikke skal vises i søkeresultatene, for eksempel pornografi. De fleste populære søkemotorer og tjenesteplattformer er utstyrt med denne type filtreringsmekanismer, men ingen av mekanismene er 100 % effektive og det er relativt enkelt å omgå begrensningene.

Praktisk sett er det også umulig å utelukke at barn blir eksponert for et uønsket innhold tilfeldig, gjennom filmer, videoklipp, bilder, kommentarer til avisartikler eller blogger. Mange plattformer tilbyr muligheter for rapportering av upassende innhold. For å gjøre tjenestene bedre bør man benytte disse mulighetene.

Bruk av Begrenset innhold-modus forutsetter at plattformene administreres av ressurser med IT-kompetanse og i dialog med pedagogisk ansvarlige, gjerne sentralt hos skoleeiere.

Filtrering av innhold på internett

En annen måte å skjerme barn for skadelig innhold er ved å bruke internettfilter. Dette er et programvareverktøy som gjør at systemadministratorer kan kontrollere listen over tillatte søkeord, og blokkere bestemte søkeord, nettsteder eller programmer/tjenester. På denne måten beskyttes barna mot tilgang til pornografisk materiale og vold på internett.

Internettfilter er et av de mest omtalte tekniske hjelpemidler for å skjerme barn fra skadelig innhold på internett og de omtales som «familiefilter», «tilgangsvakt», «innholdskontroller», «innholdsfilter» eller lignende (eng. «parental control», «internettfilter»). Man skiller mellom beskyttelse på enhetsnivå og

nettverksnivå.

Beskyttelse på enhetsnivå

De fleste innholdsfiltre fungerer på to måter. For der første fungerer innholdsfiltre ved å analysere adressen til siden som brukes laster opp (for eksempel enellerannentjeneste.com.) og sjekke om siden ble klassifisert av filterets leverandør som uønsket. Dette vil ikke virke hvis siden ikke er klassifisert i det hele tatt. I tillegg må listen med uønskede adresser vedlikeholdes kontinuerlig, noe som kan være ressurskrevende.

I tillegg kan innholdsfiltre fungere slik at innholdet på siden analyseres og kontrolleres for forbudte ord eller setninger. Dette kan føre til feil blokkering av sider (f. eks. navnet «Essex» inneholder det forbudte ordet «sex», eller sider med ordet «sex» som er ment til opplæring i seksualundervisning). Dette vil heller ikke virke for fremmedspråklig innhold, for eksempel film.

Hvis barnehage-/skoleeier velger å bruke programvare for innholdsfiltrering bør de være klar over at det er store forskjeller mellom kvaliteten på tilgjengelige løsninger. Innføring, bruk og forvaltning av innholdsfiltre krever ressurser og kompetanse samt gode administrative prosesser og rutiner som ivaretar både personvern og de pedagogiske premissene for undervisning.

Ved anskaffelse av programvare/verktøy for innholdsfiltrering, kan barnehage-/ skoleeier vurdere kvaliteten av verktøyet ved å se på følgende kriterier (sjekklisten er ikke uttømmende):

- Hvilken metode for filtrering støttes - innhold(ord), kun klassifisering av adresser eller begge metodene?
- Hvor stor er databasen med klassifiserte adresser og hvor ofte oppdateres den? Antall nettsteder og sider på internett teller i milliarder og det kommer stadig inn nye. Store databaser med klassifiserte adresser, og hyppigere oppdateringer øker kvaliteten på løsningen.
- Hvor fleksible er kriteriene for å blokkere sidene? De enkleste verktøyene skiller bare sider som er merket som gode eller dårlige, og det er produsenten som definerer kriteriene. De dyreste verktøy klassifiserer sider på klart definerte kategorier (f.eks. «narkotika», «pornografi»). I tillegg kan administrator selv definere hva som skal blokkeres og kan oppheve blokkering av nettsteder som har blitt feilaktig klassifisert.
- Tillater verktøyet å blokkere sider som ikke er klassifisert? På samme måte som

ovenfor kan mangelen på en blokkeringsfunksjon trekke ned på hvor god løsningen er.
- Gir leverandøren av filteret teknisk assistanse ved kategorisering/blokkering og oppheving av blokkering?
- Hvor enkel er tjenesten å administrere.
- Hvor godt ivaretar løsningen den enkeltes personvern.

Beskyttelse på nettverksnivå (innebygde filtre i rutere, brannmur eller innstillinger i nettverk)

Innholdsfiltrering ved tilgangen til nettverket er en av de mest effektive beskyttelsesmetodene. Fordelene med denne løsningen er:

- Mindre sjanse for at barnet deaktiverer filter selv.
- Filtreringsprogrammet er installert av nettverksadministratoren på hele nettverket og ikke på den lokale datamaskinen.
- Sentralisert filterstyringssystem (uansett om det er på nettverksnivå eller på enhetsnivå) gir som regel bedre filtreringskvalitet.

Det er forskjeller hvordan barnehage-/skoleeiere organiserer sin IT-funksjon og dermed nettverksadministrasjon. Det er viktig at eventuelle avgjørelser om innholdsfiltrering skjer i samarbeid med pedagogisk ansvarlige i kommunen/fylkeskommunen og med skolene.

De innebygde filtrene vil fungere i de nettverkene de er installert, for eksempel på skolens nettverk, men ikke utenfor skolens nettverk. Dette kan bety at mobiltelefoner eller andre mobile enheter som elever tar med på skolen og som gjerne er koblet opp mot mobilnettet ikke vil bli beskyttet. De er gjerne heller ikke beskyttet på enhetsnivå (barnehage-/skoleeiere kan ikke installere filtre på privat eide enheter). Derfor er også dialog barnehage-hjem og skole-hjem vesentlig som tiltak for skjerming mot skadelig innhold.

Begrensninger ved bruk av filter

Innholdsfiltre har tekniske begrensninger for bruken, og virker hovedsakelig ved å filtrere pornografi og vold på nettsteder og e-post. De kan ikke filtrere tjenester som p2p-programmer (person-til-person), online spill, chatter eller direktemeldinger. De kan bare blokkere dem helt. De beskytter heller ikke mot å etablere kontakter online.

Et filter som tar mye kontroll og som er vanskelig å omgå innebærer i praksis enten en overvåkning og analyse av nett-trafikken, eller overstyring av brukerens utstyr, og vil kunne føre til både sikkerhets- og personvernutfordringer.

Tiltak når barn har sett alvorlig skadelig innhold

Tekniske filterløsninger kan begrense tilgang til mye alvorlig skadelig innhold. Det er likevel en risiko for at denne type innhold blir tilgjengelig for barna. Teknisk svikt hos leverandør eller hos kunde, rutinesvikt for bruk av enheter eller ureglementert bruk av digitale enheter på mobilnettet kan være mulige årsaker. Barnehage- og skoleeiere bør utarbeide rutiner for håndtering av slike situasjoner.

Tips til håndtering:

- Ivareta barna som har fått tilgang til alvorlig skadelig innhold
- Ta barnas opplevelser på alvor og bruk tid på å snakke om det som skjedde
- Handle raskt, spredning kan skje fort
- Sørg for dokumentasjon av innholdet
- Vurder hvordan foreldre skal involveres
- Kontakt tjenesteleverandøren
- Kontakt eventuelt politiet

Det er viktig å dokumentere hendelser for å sikre at informasjon blir korrekt gjengitt. Lenker til innhold, skjermopptak og skjermbilder må lagres. Man må også vurdere om innholdet ligger innenfor eller utenfor definisjonen av alvorlig skadelig innhold.

En objektiv vurdering av innholdet vil ha betydning for videre håndtering. Samtidig er barnets oppfatning av innholdet av største viktighet.

Rutiner for håndtering bør si noe om:

- oppfølging av de involverte
- dokumentasjon
- varsling, dialog og oppfølging av foreldre

- avviksrapportering
- mediehåndtering
- anvendelse av prosedyrer i eksisterende beredskapsplaner
- eventuell kontakt med politiet

Anbefalinger og nyttige lenker

- Det innholdet barn møter på nett, i barnehagen og på skolen må være tilpasset deres nivå og ikke på noen måte fremstå skadelig for dem.
- Bruk av tilgjengelige tekniske løsninger for skjerming av barn fra skadelig internett-innhold (f. eks. filter) bør være et obligatorisk tema i risikovurderinger ved anskaffelser av utstyr, infrastruktur, digitale tjenester og ressurser, og ved valg av nettleverandører.
- I Norge har omtrent alle internettleverandørene inngått et samarbeid med Kripos og innført et nasjonalt filter som leveres og vedlikeholdes av Kripos. Dette filteret blokkerer tilgang til innhold med seksuelle overgrep mot barn, og barnehage- og skoleeiere bør vurdere å innføre det.
- Risikovurderinger og tydelige krav til sikkerhet og personvern bør stilles i kravspesifikasjoner ved anskaffelser av digitale læringsressurser, digitale læremidler, utstyr, infrastruktur og nettverk og andre digitale tjenester.
- Barnehage- og skoleeiere bør ha rutiner og retningslinjer som regulerer bruk av PC/nettbrett og annet utstyr med tilgang til internett. Disse bør være konkrete og bør ta hensyn til lokale behov og bestemmelser. De må oppdateres med jevne mellomrom og må kommuniseres til alle involverte parter, også foreldre.
- Barnehage- og skoleeiere bør vurdere å installere filtre på digitale enheter for barn i barnehagealder og elever på 1.- 4. årstrinn.
- Hvis barnehage- og skoleeiere velger å bruke internettfiltre eller andre tekniske løsninger bør de gå i dialog med foreldre og anbefale å sikre barn hjemme og i mobilnettet med samme typer filtertjenester.
- Fokus på digital kompetanse hos barn og ansatte, og dialog med foreldre må være en kontinuerlig prosess i tråd med teknologiutvikling. Prosessen bør forankres i gode rammeverk som profesjonsfaglig digital kompetanse for lærere, digitale ferdigheter som definert i læreplaner og bestillerkompetanse hos barnehage- og skoleeiere som sikrer profesjonelle IT-anskaffelser.

Nyttige lenker

Dubestemmer.no - en nettressurs om personvern, nettvett og digital dømmekraft

Medietilsynet - om barn og medier

Nettvett.no - informasjon, råd og veiledning om sikrere bruk av internett

Grunnprinsipper for IKT-sikkerhet - en veiledning fra Nasjonal sikkerhetsmyndighet

Udir.no - Skolemiljøtiltak - elevens digitale liv

Tilgang, bruk, risiko og muligheter – norske barn på Internett. Resultater fra EU Kids Online-undersøkelsen i Norge 2018