



Oslo

Der unge er bør også kommunalt ansatte være

Oppsøkende arbeid via digitale aktiviteter – gaming



SALT

SAMMEN LÅGER VI ET TRYGT OSLO

1 Vurderinger i forkant av kommunens tilstedeværelse på nett

I tillegg til å sette seg inn i relevante lovverk er det flere vurderinger som må gjøres i forkant av tilstedeværelse på nett. En av vurderingene er tilknyttet personopplysningsloven.

Personvern vurderinger

Den kommunale virksomheten er ansvarlig (se boksen om «Behandlingsansvar» under) for at behandlingen av personopplysninger i tilstedeværelsen på nett etterlever personopplysningsloven (Kommunesektorens Organisasjon, 2022). Hver bydel har ansatt en personvern - og informasjonskoordinator som kan kontaktes for råd og veiledning. I forkant av tilstedeværelse på gamingplattformer og behandling av personopplysninger må virksomheten derfor gjennomføre vurderinger av personvern, også når det er usikkert om det er nødvendig.

Ungdommene som oppholder seg mye på gamingplattformer er ikke nødvendigvis vant til å møte på sosioarbeidere eller andre kommunalt ansatte på disse plattformene. Når man er til stede på nettet er det derfor viktig at man

Behandlingsansvar

En behandlingsansvarlig er ethvert organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger, samt hvilke midler som skal benyttes.

Det er ofte leverandørene av plattformene som har behandlingsansvar for store deler av behandlingen, basert på egne formål. Virksomhetene vil imidlertid etter avtale med leverandørene kunne ta i bruk plattformene for egne formål. Ettersom at formålene ofte innebærer behandling av personopplysninger, medfører dette at også virksomhetene har behandlingsansvar.

Den behandlingsansvarlige har ansvar for at:

1. Behandlingen av personopplysninger etterlever personopplysningsloven.

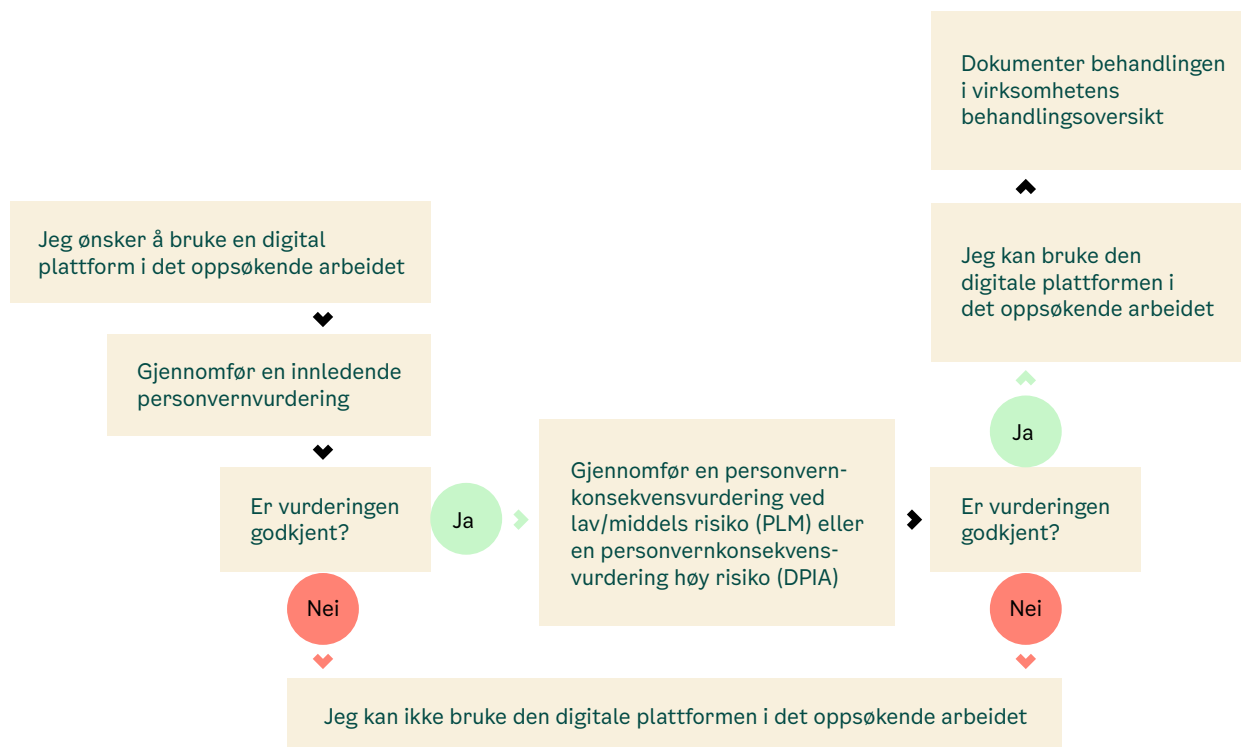
Det er den behandlingsansvarlige som har det overordnede ansvaret for at behandlingen etterlever personopplysningsloven, herunder personvernprinsipper og de registrertes rettigheter.

2. Behandlingen av personopplysninger har et behandlingsgrunnlag.

Det er den behandlingsansvarlige som har ansvaret for at behandlingen har et behandlingsgrunnlag. For oppsøkende arbeid på digitale plattformer er det særlig to aktuelle behandlingsgrunnlag, henholdsvis utøvelse av offentlig myndighet og berettiget interesse.

Dersom leverandøren av plattformen tilhører et land utenfor EU/EØS som ikke er på EU's liste over godkjente land, må virksomheten i tillegg til et behandlingsgrunnlag også ha et overføringsgrunnlag. Virksomheten bør også forsikre seg om at det ikke finnes lover eller praksiser i det aktuelle landet som til tross for et overføringsgrunnlag vil medføre at personvernloven ikke etterleveres i praksis.

Hva må virksomheten gjøre i forkant av tilstedeværelse på nett?



Modellen er utarbeidet etter inspirasjon fra [modellen til KS](#) (som du finner på [denne lenken](#)).

Først må virksomheten gjennomføre en [Innledende personvern-vurdering \(IP\)](#). Vurderingen kartlegger informasjon om en behandling av personopplysninger, og vurderer på bakgrunn av informasjonen risikoen for den registrerte som virksomheten behandler opplysninger om. Risikovurderingen omfatter risiko knyttet til [personvernprinsippene](#) og den registrertes [rettigheter](#) (Kommune-sektorens Organisasjon, 2022).

Gjennomføringen av en vurdering av personvernkonsekvenser bør gjøres av en gruppe sammensatt av personer med ulik faglig bakgrunn. I spørsmål som omhandler sosiale medie- og gamingplattformer kan nyttige samarbeidsaktører være ansatte fra kommunikasjonsfaget.



På bakgrunn av risikovurderingen i en Innledende personvern-vurdering (IP), må virksomheten gjennomføre en Personvernkonsekvensvurdering ved lav/middel risiko (PLM) eller en Personvernkonsekvensvurdering ved høy risiko (DPIA). Antakelig vil tilstedeværelse på nett medføre en høy risiko for personvern-prinsipper og rettigheter, men virksomheten må likevel vurdere hvert enkelt

tilfelle konkret. Risikoen kan nemlig tenkes å variere mellom de ulike måtene å være til stede på nett (Kommunesektorens Organisasjon, 2022). Dersom det er behov for råd og veiledning med utfylling av DPIA kan bydelens personvern og informasjonskoordinator kontaktes.

En vurdering av personvernkonsekvenser (enten en PLM eller en DPIA), og konklusjonen av denne vurderingen, skal forankres i ledelsen i den kommunale virksomheten. Det vil si at ledelsen beslutter og begrunner ett av de følgende alternativene:

1. **Godkjenning.** Vurderingen av personvernkonsekvenser er godkjent. Virksomheten kan ta i bruk digitale plattformer i oppsøkende arbeid på nett.
2. **Betinget godkjenning.** Vurderingen av personvernkonsekvenser godkjennes under forutsetning av følgende forbedringer... (beskriv forbedringene). Revidert vurdering av personvernkonsekvenser skal fremlegges for ledelsen på nytt.
3. **Ikke godkjent.** Vurderingen av personvernkonsekvenser er ikke godkjent. Virksomheten kan ikke ta i bruk digitale plattformer i oppsøkende arbeid på nett.

Før virksomheten kan behandle personopplysninger, må behandlingen dokumenteres i virksomhetens behandlingsoversikt (Kommunesektorens Organisasjon, 2022). Oslo kommune har et felles system (se [Behandlingsoversikten](#)) for å dokumentere alle behandlinger av personopplysninger.

Sikkerhet

Ved opprettelse av en sosial mediekonto bør virksomheten foreta grundige vurderinger knyttet til sikkerhet.

To-trinnssertifisering og sterke passord bør benyttes.

Anbefalinger for sikring av konto og passord kan eksempelvis finnes hos NSM¹ og Nettvett². Flere enheter kan som regel legges til med MFA (multi factor authentication) på samme bruker dersom det er behov for at flere personer har tilgang til brukeren. Generelt sett anbefales det å ikke dele fellespassord over «klare» kanaler, som Teams, E-post og lignende. Bruk av passordvelv³ eller andre krypterte kanaler anbefales.

[1] <https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord>

[2] <https://nettvett.no/passord/>

[3] <https://bitwarden.com/>

Rolle knyttet til gaming

Gjennom tilstedeværelse i gaming kan kommunalt ansatte innta en mer eller mindre uformell rolle i møte med ungdom. Dette blant annet på grunn av fokuset på etablering av kontakt og relasjon med ungdom gjennom interaksjon, eksempelvis i form av chatting via gaming (se kapittel «Kommunalt ansattes tilstedeværelse på nett»).

Ungdommene som oppholder seg mye på gamingplattformer er ikke nødvendigvis vant til å møte sosialarbeidere eller andre kommunalt ansatte på disse plattformene. Når man er til stede på nettet er det derfor viktig at man er tydelig i rollen som kommunalt ansatt.



Hvordan synliggjøre kommunalt ansatte sin rolle:

- › Ikke bruke private profiler.
- › Tydelig avsender: Bruke profiler med navn tilknyttet den kommunale virksomheten man representerer (for eksempel «Utekontakten Bydel XX»), og med kommunevåpen som profilbilde. På den måten signaliseres tydelig at man representerer en kommunal virksomhet.
- › Gjøre ungdom kjent med hvem man er, hvilke hensikter man har med arbeidet og ikke minst hvilke regler (herunder informasjon om for eksempel taushetsplikt, avvergingsplikt og opplysningsplikt) som ligger til grunn for arbeidet.
- › Synliggjøre hvem i virksomheten som er pålogget på den aktuelle plattformen, samt kontaktinformasjon til virksomheten.
- › Reflekter over hvordan man benytter emoji's og memer i dialog med ungdomsmiljøet og hvordan det kan fortolkes av mottaker.
- › Legg inn autosvar ved henvendelser på chat/melding om åpningstider i tidsrom plattformen ikke er betjent med kontaktinformasjon til andre akutte tjenester.

Gaming plattform(er)

Det finnes mange plattformer å velge mellom når man skal arbeide oppsøkende på nett. Når man skal velge plattform, er det viktig at man:

- › Finner ut hvilke(n) plattform(er) ungdommene er på.
- › Bestemmer seg for en plattform man ønsker å arbeide oppsøkende på (man kan arbeide på flere eller andre plattformer etter hvert).
- › Setter seg inn i plattformen, som for eksempel hvem som bruker den, hvordan den fungerer og ikke minst hvilke regler som finnes for bruk av den (dette er viktig for å vurdere om det er en plattform man kan arbeide oppsøkende på).

Forankring

Det er viktig at tilstedeværelse på nett ikke blir et personlig ansvar liggende utenfor den kommunale virksomhetens ordinære arbeid. Før virksomheten starter tilstedeværelsen på nett bør man:

- › **Forankre arbeidet**

Den kommunale virksomheten bør forankre arbeidet på nett hos nærmeste leder. Forankringen gir legitimiteten som er nødvendig for arbeidet.

- › **Involvere samarbeidspartnere i arbeidet**

Den kommunale virksomheten bør involvere samarbeidspartnere i det kommunens tilstedeværelse på nett. Ofte fører arbeidet til avdekking av behov for ulike tiltak, og økonomien og ansvaret for tiltakene kan være hos samarbeidspartnere. For å ansvarliggjøre samarbeidspartnere kan den kommunale virksomheten opprette en referansegruppe som møtes jevnlig. Da kan samarbeidspartnere få et større eierforhold til tilstedeværelsen på nett, og dermed et større ansvar for eventuelle tiltak.

Forankring er også viktig i andre deler av tilstedeværelsen på nett. Se kapittel 3 om «Vurderinger i forkant av kommunens tilstedeværelse på nett» for viktigheten av å forankre en vurdering av personvernkonsekvenser i ledelsen.

I forkant av tilstedeværelse på sosiale medie- og gamingplattformer og behandling av personopplysninger må virksomheten gjennomføre vurderinger av personvern, også når det er usikkert om det er nødvendig.



Utfordringer med tilstedeværelse på nett

Tilstedeværelse på nett, både ved kartlegging av ungdomsmiljøer og ved etablering av kontakt og relasjon med ungdommer, kan ha visse utfordringer. Det er viktig at offentlige ansatte er bevisst de utfordringer som ligger i oppsøkende arbeid på nett.

Anonymitet

Mulighet for anonymitet kan for mange ungdommer medføre lavere terskel for å etablere kontakt med kommunalt ansatte. Når det er sagt kan anonymitet også medføre flere utfordringer. Gjennom oppsøkende arbeid kan man få informasjon som bekymrer. Et eksempel kan være at du som kommunalt ansatt blir bekymret for en ungdom som på en av plattformene kommuniserer at han eller hun vil begå selvmord. Utfordringen oppstår dersom denne ungdommen er anonym, ettersom man da har få eller ingen opplysninger som kan identifisere vedkommende. Dersom man kommuniserer med en anonym ungdom og det fremkommer informasjon som innebærer akutt fare for liv eller helse, er politiet den aktøren man skal ta kontakt med. Politiet har større mulighet enn kommunalt ansatte til å identifisere og hjelpe ungdommen.

Usikkerhet rundt hvem vi snakker med

I forbindelse med anonymitet er det relevant å nevne at kommunalt ansatte aldri kan vite helt sikkert hvem de kommuniserer med på nett. Det samme er tilfellet for ungdommene. En mulighet for å sikre kommunikasjonen mellom partene, er at man avtaler et passord eller en kode som bare den kommunalt ansatte og den aktuelle ungdommen kjenner til. Da kan partene, i større grad, være sikre på at de kommuniserer med rett person.

Ikke dele sensitiv informasjon

En annen mulighet for å sikre kommunikasjonen mellom partene, er at man ikke deler sensitiv informasjon på nett. Kommunalt ansatte bør oppfordre ungdommene til det samme. Også når man er sikker på hvem man kommuniserer med, er det viktig at man ikke deler sensitiv informasjon. Dette fordi andre parter, som for eksempel eier av plattformene, kan få tilgang til den informasjonen som kommuniseres mellom den kommunalt ansatte og den aktuelle ungdommen.

Politiet har i sin digitale kommunikasjon med publikum tatt i bruk sikker chat. Kontakten blir til via politiets plattformer på sosiale medier. Deretter vil de som kontakter politiet motta en lenke som leder til sikker chat. Chatrommet er kryptert og man mottar et kodeord for å kommunisere videre med politiet. Slik sikres personvern og sikkerhet rundt sensitive opplysninger.



Vurdering av informasjon

Nettet kan gi et feilaktig bilde av virkeligheten, og dermed også et feilaktig bilde av ungdom og ungdomsmiljøer. Fremveksten av kunstig intelligente systemer, som for eksempel ChatGPT, gjør at kommunalt ansatte bør være ekstra påpasselig på dette. Slike systemer kan overøse nettet med informasjon i form av eksempelvis bilder, videoer, lyd og tekst (Bogen, 2023).

Begrenset mulighet

Noen ungdommer opplever begrenset mulighet for digital deltakelse (se rapporten til Redd Barna for mer informasjon). Dette på grunn av barrierer som for eksempel dårlig tilgang på nett og digitale tjenester, manglende foreldre-støtte, mobbing og hatprat på nett samt levekår og boforhold (Redd Barna, 2022). Som følge av slike barrierer finnes det noen ungdommer man ikke vil nå gjennom tilstedeværelse på nettet, og som man derfor må fortsette å søke og nå gjennom oppsøkende arbeid på gaten.

Begrenset tilgjengelighet

Kommunalt ansatte er ikke tilgjengelige hele døgnet. Dette gjør at ungdom kan befinne seg i situasjoner uten tilgang til hjelp og støtte fra kommunalt ansatte. I slike situasjoner er det viktig at ungdom er informert om andre hjelpetjenester som de kan kontakte i stedet. Ikke minst er det viktig at ungdom i slike situasjoner er informert om når kommunalt ansatte faktisk er tilgjengelige, slik at ungdommene vet når de kan kontaktes og ikke. En måte å gjøre dette på er å tydeliggjøre åpningstiden til den kommunale virksomheten på de sosiale medie- og gamingplattformene som virksomheten bruker.

Sikkerhet

Selv om tjenesten følger sikkerhetsmessige råd vil det alltid være et rom for at en konto kan bli hacket eller informasjon kommer på avveie. Det er derfor nødvendig å minimere risiko for dette så langt det lar seg gjøre.

To-trinnssertifisering og sterke passord bør benyttes.

Man kan oppleve at man ikke klarer å etablere kontakt med ungdom, men likevel gjøre viktige observasjoner. Å beskrive det man observerer i et ungdomsmiljø, i dette tilfellet på en digital plattform, er også en viktig oppgave i det forebyggende arbeidet. Beskrivelsene kan brukes til å «ta pulsen» på ungdomsmiljøet (Oslo kommune, 2020). En viktig presisering er at kommunalt ansatte jobber i åpne kilder og sammenfatter kunnskap fra den informasjonen som ligger offentlig tilgjengelig på nettet.



3 Hva gjør jeg dersom jeg avdekker noe bekymringsfullt på nett?

Når man arbeider på digitale plattformer, kan man avdekke bekymringsfull atferd. I slike tilfeller kan man ha en plikt til å avverge atferden og/eller en plikt til å opplyse om atferden.

Det er viktig å presisere at dette kan være ytringer eller materiale som er fremsatt **direkte** til kommunen i chat eller liknende eller som ansatte i kommunen **kan komme over** som følge av tilstedeværelse på nett.

En offentlig ytring defineres etter Straffeloven § 10 slik:

§ 10. Offentlig sted og offentlig handling

Med offentlig sted menes et sted bestemt for alminnelig ferdsel eller et sted der allmennheten ferdes.

En handling er offentlig når den er foretatt i nærvær av et større antall personer, eller når den lett kunne iakttas og er iakttatt fra et offentlig sted. Består handlingen i fremsettelse av en ytring, er handlingen også offentlig når ytringen er fremsatt på en måte som gjør den egnet til å nå et større antall personer.

Dersom ytringen kommunen kommer over på nett har et omfang som når flere enn 20-30 personer anses den som offentlig. Det betyr at denne informasjonen ikke er underlagt taushetsplikt som utgangspunkt. I praksis betyr det at utekontakter og andre kan benytte denne informasjonen som om det ble fremsatt i et offentlig rom. Likevel må det presiseres at det må foretas en vurdering fra tilfelle til tilfelle. Fremstår det som er lagt ut som bevisst og ønsket spredd offentlig?

Eksempel på det motsatte kan være en screenshot eller innhold som spres uten at den det gjelder har samtykket til det.

Utekontakter og andre som jobber med ungdom må derfor vurdere hvorvidt informasjon som når flere enn 20-30 kan brukes i det sosialfaglige arbeidet.

Avvergingsplikt

Kommunalt ansatte har en plikt til å avverge lovbrudd (straffeloven, 2005, § 196).

Avvergingsplikten (strl. § 196)

Med bot eller fengsel inntil 1 år straffes den som unnlater å anmelde til politiet eller på annen måte å søke å avverge et lovbrudd eller følgene av det, på et tidspunkt da dette fortsatt er mulig, og det fremstår som sikkert eller mest sannsynlig at lovbruddet er eller vil bli begått. Avvergelsesplikten gjelder uten hensyn til taushetsplikt og innebærer en plikt til å avverge en rekke lovbrudd. Se [strl. § 196](#) for mer informasjon.



Case:

Fritidsklubben i bydelen har opprettet en Discord server og en av de ansatte har ansvar for modereringen. Utpå kvelden dukker det plutselig opp en bombeemoji i kommentarfeltet og følgende bilde:

Den ansatte ved fritidsklubben vet hvem brukeren er. Ungdommen har tidligere delt drøye bilder/memer på nett tidligere.



Hva bør den ansatte gjøre i denne situasjonen?

Case:

Under en gaming-kveld på fritidsklubben arrangert av Utekontakten blir temperaturen og engasjementet høyt.

Utekontakten deltar selv i gamingen og alle deltakerne bruker gaming mikrofoner slik at de kan kommunisere med hverandre underveis i spillet.

I tillegg har spillet en chatfunksjon. Underveis i spillet tiltar kommunikasjonen med deltakerne seg opp. De hauser hverandre opp og når det ene laget taper poeng i kampen mot det andre laget utbryter en «Jævla n****! Du drepte meg!» og en annen følger opp med «Ta den jævla hora!». Samtidig sendes det emojis og memer i chatten. Flere ler.

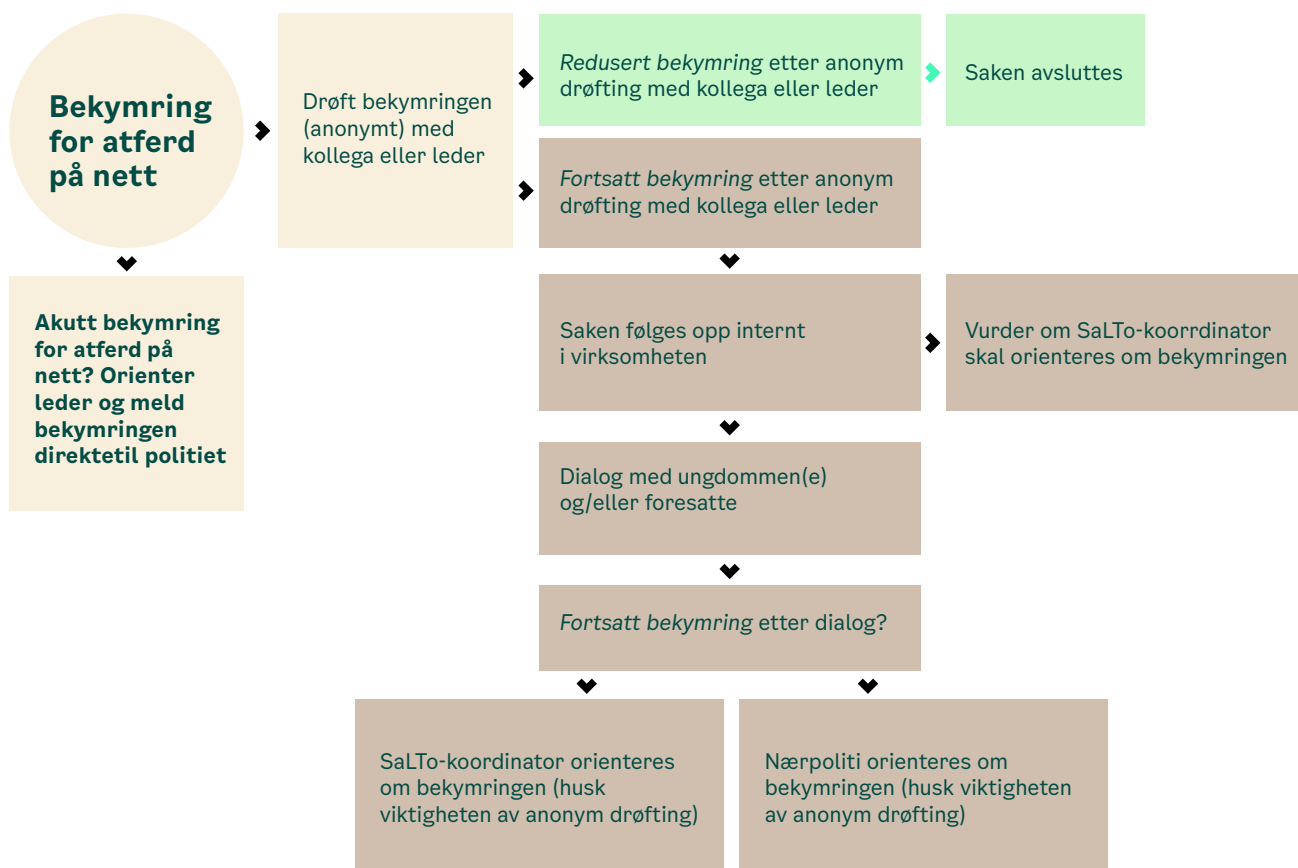
Hva bør Utekontakten gjøre i situasjonen?

Hvordan bør dette følges opp i etterkant?

Hvordan kan kommunalt ansatte gå frem dersom de er bekymret?

Under følger to modeller for hvordan kommunalt ansatte **kan** gå frem dersom de er bekymret for atferd på nett.

Trinnvis modell ved bekymringsfull atferd på nett



Med bekymring for atferd henspeiler veilederen til atferd som ikke utgjør en fare for liv og helse, og som derfor kan håndteres over tid. Med akutt bekymring for atferd henspeiler derimot veilederen til atferd som kan utgjøre en fare for liv og helse, og som derfor må håndteres akutt.

Er du bekymret for fare for liv og helse:
Ring politi: 112 eller medisinsk nødhjelp: 113.

Trinnvis modell for å tipse politiet ved bekymringsfull atferd på nett



En av fordelene med å tipse politiet er at det da er politiet som tar en vurdering av atferden man opplever som bekymringsfull.

Opplysningsplikt

Foruten en plikt til å avverge kan kommunalt ansatte også ha en plikt til å opplyse om bekymringsfull atferd. Når man arbeider på nett, både når man kartlegger ungdomsmiljøer og når man etablerer kontakt og relasjon med ungdom i miljøene, kan man avdekke bekymringsfull atferd som utløser en plikt til å opplyse for eksempel foreldre (se [forvaltningsloven](#)) eller barneverntjenesten (se [barnevernsloven](#)).

