



Retningslinjer nettundervisning og personvern

Innhold

Sammendrag/hovedbudskap	2
Generelt om personvern og informasjonssikkerhet	2
Noen sentrale begreper	2
Informasjonssikkerhet.....	2
Personopplysninger.....	2
Sensitive personopplysninger (særlige kategorier).....	3
Behandlingsgrunnlag.....	3
Ansvarsfordeling UTD og skoler	4
Rettlinjer nettundervisning.....	5
Streaming	5
Opptak av nettundervisning som elever deltar på.....	5
Hva elevene selv kan gjøre dersom de ikke ønsker å være identifiserbare i et opptak.....	5
Hva lærer kan gjøre dersom de ikke ønsker å innhente samtykke (når samtykke kreves).....	5
Informasjon til elever i forkant av opptak.....	5
Når samtykke er ikke nødvendig.	6
Når samtykke kreves	6
Elever som gjør opptak av undervisningen	6
Vedlegg 1: Begrepsforklaring	7

Sammendrag/hovedbudskap

Hovedbudskap:

- I forhold til personvern er det stor forskjell på om det gjøres opptak eller ikke av nettbasert undervisning hvor elever kan identifiseres via lyd eller bilde.
- Nettbasert undervisning uten opptak krever ikke samtykke fra elever, og lærere kan kreve at elever slår på kamera med lyd og bilde.
- Nettbasert undervisning med opptak krever heller ikke samtykke, men elever må opplyses om at opptaket skjer og få muligheten til ikke å delta eller slå av egen lyd og bilde.
- Opptak av nettundervisning som skal publiseres (utenfor klassen) krever samtykke fra alle elevene som kan identifiseres via lyd eller bilde. Samtykkeskjema må fylles ut og samles inn/arkiveres.
- Opptak av nettundervisning med elever skal kun lagres i systemer TRFK har støtte for og har databehandleravtaler med.
- I forbindelse med Covid-19 og nedstenging av skoler forventes det at alle lærere jevnlig kommuniserer med sine elever via nettundervisning og TRFKs videokonferanseverktøy.

De viktigste anbefalingene:

- Til tross for at lærer kan kreve at elever slår på kamera med lyd og bilde når klassen/gruppen har undervisning uten opptak, anbefaler vi at elevene får velge selv om de vil ha på kameraet.
- Når elevene individuelt skal ha foredrag/framlegg eller demonstrere i praktiske fag, er det rimelig å kreve at elevene slår på kamera med lyd og bilde.

Generelt om personvern og informasjonssikkerhet

Vi forbereder oss på at vi også skoleåret 2020/21 må regne med at deler av undervisningen vil foregå på nett, og har med tanke på dette laget denne veilederen for hvordan det skal foregå for å ivareta informasjonssikkerhet og personvern.

Noen sentrale begreper

En mer utfyllende begrepsliste finnes som vedlegg til dette dokumentet.

Informasjonssikkerhet

Sikring av opplysninger ved å bruke prinsippene om konfidensialitet, integritet og tilgjengelighet.

- *Konfidensialitet* – at informasjonen ikke blir kjent for uvedkommende.
- *Integritet* – at informasjonen ikke blir endret utilsiktet eller av uvedkommende.
- *Tilgjengelighet* – at informasjonen er tilgjengelig for autoriserte ved behov.
- *Robusthet* – at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser.

Personopplysninger

Opplysning eller vurdering som kan knyttes til en enkeltperson. Dette kan f.eks. være:

1. Navn, alder og fødselsnummer.
2. Adresse.
3. Telefonnummer og e-postadresse.
4. Opplysninger om elevenes underveis- og sluttevalueringer.



5. Fravær og anmerkninger.
6. Faglig progresjon.
7. Spesielle undervisningsbehov.
8. Atferdsmønstre og sosiale evner.
9. Kommunikasjon mellom elever.
10. Kommunikasjon mellom lærer og elev.
11. Informasjon om allergier.
12. Logg fra elevenes bruk av skolens nettverk.
13. Bilder, videoer eller lydfiler av elever.

Der vi genererer lister som inneholder store mengder ikke-sensitive personopplysninger, f.eks. en klasseliste med navn, e-post, telefonnummer o.l., skal denne behandles som sensitiv. Elevlister skal som hovedregel ikke utleveres til eksterne uten at det foreligger en databehandleravtale. I de fleste tilfeller vil utlevering av elevlister kreve at elevene har samtykket til utleveringen.

Sensitive personopplysninger (særlige kategorier)

I loven er det definert en rekke kategorier av opplysninger som det skal mer til å kunne behandle enn andre opplysninger (artikkel 9 og 10 i forordningen):

1. Opplysninger om rasemessig eller etnisk opprinnelse.
2. Opplysninger om politisk oppfatning.
3. Opplysninger om religion.
4. Opplysninger om filosofisk overbevisning.
5. Opplysninger om fagforeningsmedlemskap.
6. Genetiske opplysninger.
7. Biometriske opplysninger med det formål å entydig identifisere noen.
8. Helseopplysninger.
9. Opplysninger om seksuelle forhold.
10. Opplysninger om seksuell legning.
11. Opplysninger om straffedommer.
12. Opplysninger om lovovertridelser.

Behandlingsgrunnlag

For å kunne behandle personopplysninger må man ha et behandlingsgrunnlag. Disse er delt mellom situasjoner der vi har nødvendighetsgrunner og situasjoner der vi har et skriftlig samtykke.

Nødvendighetsgrunner

Behandling av personopplysninger er lovlig når det er nødvendig for:

1. Å oppfylle avtale med den registrerte.
2. Å oppfylle en rettslig forpliktelse.
3. Beskyttelse av vitale interesser.
4. Utøvelse av offentlig myndighet eller for å utføre oppgave i offentlig interesse.
5. Berettigede interesser som overstiger den registrertes rett til personvern (interesseavveining).

For alle andre behandlinger kreves det et samtykke.

Samtykke

For at et samtykke skal være gyldig, kreves det:



- At det er basert på frivillighet.
- At det er spesifikt.
- At det er informert.
- At det er utvetydig.
- At det er gitt gjennom en aktiv handling.
- At det er dokumenterbart.
- At det er mulig å trekke tilbake like lett som det ble gitt.

Vi vil i løpet av skoleåret 2020/21 ha på plass en egen løsning for å hente inn samtykke.

Ansvarsfordeling UTD og skoler

Våren 2020 lærte vi å ta i bruk digitale verktøy i undervisningen i et omfang ingen av oss var forberedte på. Dette gav oss både muligheter og utfordringer. Selv om situasjonen var og er ekstraordinær, må vi forholde oss til blant annet personvernloven, og ikke ta i bruk enkle gratisløsninger som ikke tilfredsstillende ansatte og elevers personvern. Vi har allerede systemer som dekker det som er behovet, og vi legger fortløpende ut veiledere til lærerne.

Det følgende er i all hovedsak basert på sluttokumentet til arbeidsgruppen som har sett på personvern innen Avdeling utdanning, med et særlig blikk på skolene. Formålet med arbeidet var å klargjøre rutiner, roller og ansvar når det gjelder informasjonssikkerhet og personvern for all bruk av IKT-systemer på Avdeling utdanning. Rutinene er begrenset til de IKT-systemene som finansieres og administreres av Avdeling utdanning eller den enkelte skole.

Avdeling utdanning har ansvar for at alle rutiner rundt bruken av IKT-systemer hvor systemeierskapet er tildelt en av seksjonslederene på avdelingen. Dette gjelder blant annet Everyday, Canvas og vigofamilien.

Rektor har ansvar for at alle IKT-systemer som skolen selv finansierer og/eller bruker i stedet for eller som supplement til avdelingens systemer.

Ansaret består i å sikre at bruken av systemet er i henhold til enhver tid gjeldene lovverk og interne regler som gjelder informasjonssikkerhet og personvern. Dette innebærer blant annet ansvaret for at behandlingsprotokoll og databehandleravtaler er korrekte.

Informasjon til elevene om undervisning, vurdering, skolehverdag etc. skal foregå i IKT-systemer anskaffet / finansiert og tilrettelagt av Trøndelag fylkeskommune. Sosiale medier kan brukes som supplement, men ikke som eneste kanal. Det oppfordres til å ikke benytte sosiale medier som informasjonskanal til elever overhode.

Vi har laget en enkel punktliste som vi ber skolene forholde seg til:

1. Elevene eier sine egne datamaskiner og er selv ansvarlig for hva de installerer på disse.
2. Elevene skal læres opp til å være bevisst på hva slags data de legger igjen; hva som skjer med dem, hvem som eier dataene og hvordan de eventuelt kan brukes av andre.
4. Lærere skal ikke kreve at elever må ta i bruk gratisprogrammer som ikke er anskaffet og tilrettelagt av Trøndelag fylkeskommune. Programvare som finnes i Skoleportalen og i Canvas er godkjent av skoleeier og skal være i henhold til gjeldende personvernlovgiving. Det oppfordres til at disse brukes som hovedregel.
5. Lærere skal være ekstra varsomme med å oppfordre til bruk av gratisprogrammer hvor elevene må opprette brukerkonto eller hvor personopplysninger registreres, ref. punkt 2.
6. Fagsystemer og programvare anskaffet av skoleeier skal brukes til digital kommunikasjon med elevene.



7. Lyd- og videoopptak av elevene skal ikke gjøres uten deres samtykke.

Dersom det dukker opp ønsker om annen programvare enn det vi disponerer i dag, ber vi om at skolen ved rektor tar kontakt med seksjonsleder eksamen og digitalisering.

Retningslinjer nettundervisning

Retningslinjene gjelder for alle som utfører digital undervisning ved i Trøndelag fylkeskommune. Lærer må være spesielt oppmerksomme på at publiserte opptak ikke inneholder taushetsbelagte personopplysninger. Unngå å inkludere sensitive personopplysninger i undervisninger og opptak.

Dersom det er nødvendig, ta kontakt med personvernombudet@trondelagfylke.no, eller andbj@trondelagfylke.no.

Streaming

Ved streaming av undervisning er det i utgangspunktet frivillig for elever om de ønsker å delta med bruk av bilde og / eller lyd under strømmingen av undervisning. Dette styres av eleven med innstillinger ved tilkoblingen til undervisningsstrømmen, og kan også når som helst endres av elever så lenge strømmingen foregår.

Opptak av nettundervisning som elever deltar på

Lærer vil i oppstarten av nettundervisningen informere om at opptak vil bli gjort. Opptaket kan omfatte bilde, lyd, lærers foiler og / eller video der lærer og foilene er i fokus, men med mulighet for at bilde / video og / eller stemmen til elever blir med i opptaket.

Hva elevene selv kan gjøre dersom de ikke ønsker å være identifiserbare i et opptak

Elever kan ikke reservere seg fra å delta i nettundervisning. Deltakelse i slik undervisning truer ikke elevenes personvern.

Generelt bør elevene kunne velge om de har på kameraet der klassen/gruppen har undervisning. Vi skjønner at ikke alle vil vise fram hjemmet sitt.

Der elevene individuelt skal ha foredrag/framlegg, demonstrere i praktiske fag, kan vi kreve at elevene slår på kameraet. Dette er konkrete vurderingssituasjoner som handler om muligheten til å få standpunktvurdering.

Hva lærer kan gjøre dersom de ikke ønsker å innhente samtykke (når samtykke kreves)

- Lærer kan lage forelesningsvideoer som vedkommende produserer uten at andre deltar i videoen. Lærer kan samtykke til opptak ved å selv starte opptak.
- Lærer kan ta pauser i opptaket der elevene gis anledning til å stille spørsmål.
- Dersom det gjøres opptak der lærer baserer seg på at elevene slår av mikrofon/kamera osv., må lærer gjennomgå opptaket i etterkant for å forsikre seg om at personopplysninger ikke vises i opptaket. Eventuelt kan samtykke innhentes fra kun de elevene som er identifiserbare.

Informasjon til elever i forkant av opptak

Denne informasjonen kan gis i Canvas, og lærer må minne elevene på at det gjøres opptak.

Formålet med opptaket er å gjøre nettundervisningen tilgjengelig for elevene som er forhindret fra å følge undervisningen i sanntid.

Opptak publiseres som en læringsressurs i Canvas og vil være tilgjengelig for alle elever i det aktuelle faget. Opptak der elever er identifiserbare skal lagres på et sikkert sted så lenge de er faglig relevante. Et opptak skal slettes når formålet med opptaket er oppfylt. Som regel er dette når eksamen er gjennomført.

Dersom opptakene skal brukes til et annet formål (kvalitetssikring, forskning, læringsanalyse etc.), må det innhentes samtykke fra de som er med på opptaket.

Når samtykke er ikke nødvendig.

For undervisning der det er essensielt for å oppnå formålet med undervisningen at elever deltar aktivt, vil det anses å være av allmennhetens interesse å behandle personopplysningene til deltakerne i undervisningen. Dermed vil behandlingsgrunnlaget være hjemlet i GDPR art. 6 nr. 1 bokstav e. I dette tilfellet kreves ikke samtykke fra elever. Men elever har mulighet for å skjerme seg ved å bruke metoden ovenfor.

Når samtykke kreves

Ved opptak av andre typer undervisning, kreves samtykke fra elever som er identifiserbare i opptaket (jfr. GDPR art 6 nr. 2 bokstav a). Det må vurderes om lærers behov for å gjøre opptak er strengt nødvendig for å oppfylle formålet med utdanningen. I dette ligger at opptak må være egnet for å nå formålet. Hvis det ikke er nødvendig å ta opptak for å oppfylle elevenes rettigheter og skolens forpliktelser, skal det i utgangspunktet ikke gjøres.

Elever vil i så fall bli bedt om å gi sitt samtykke. Samtykket kan trekkes tilbake. Tilbaketrekning av samtykke må skje skriftlig til administrasjonen ved skolen. Dersom en elev som er identifiserbar i opptaket, ikke samtykker eller trekker sitt samtykke, må opptaket redigeres/slettes. Dette gjelder ikke dersom det er kun bilde som vises, og opptaket kun publiseres som en læringsressurs i Canvas for elever som deltar i samme fag. I slike tilfeller kan bruk av bilde hjemles i åndsverksloven.

Elever som gjør opptak av undervisningen

Hvis elever ønsker å gjøre egne opptak, kan dette ikke distribueres i strid med åndsverkloven. Dette betyr at opptaket kun kan være til eget bruk, og ikke kan deles med noen.

Dersom elever har et nødvendig behov for å dele opptak med medelever som ikke har hatt anledning til å delta i undervisningen, må man ta kontakt med lærer for å få samtykke til dette. I tillegg må det innhentes samtykke fra eventuelle medelever som er identifiserbare i opptaket.

Vedlegg 1: Begrepsforklaring

Autentisering: Handling for å bekrefte identitet (person / organisasjon).

Behandlingsansvarlig: Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Dette er vanligvis en virksomhet.

Behandling av personopplysninger: All bruk av personopplysninger, slik som innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter.

Behandlingsgrunnlag: Rettslig grunnlag for å behandle personopplysninger. Dette kan for eksempel være samtykke.

Databehandler: Den som behandler personopplysninger på oppdrag fra den behandlingsansvarlige. Dette er vanligvis en virksomhet.

Databehandleravtale: En avtale mellom databehandler og behandlingsansvarlig om hvordan personopplysninger skal behandles.

Dataminimering: Prinsipp om at innsamling av data skal avgrenses til det som er strengt nødvendig for å oppnå formålet.

Den registrerte: Enkeltpersonen som de lagrede opplysningene kan knyttes til.

DPIA: Forkortelse for Data Protection Impact Assessment, en vurdering av personvernkonsekvenser. En prosess som skal bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreducerende tiltak.

Informasjonssikkerhet: Sikring av opplysninger ved å bruke prinsippene om konfidensialitet, integritet og tilgjengelighet.

- *Konfidensialitet* – at informasjonen ikke blir kjent for uvedkommende.
- *Integritet* – at informasjonen ikke blir endret utilsiktet eller av uvedkommende.
- *Tilgjengelighet* – at informasjonen er tilgjengelig for autoriserte ved behov.
- *Robusthet* – at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser.

Konfidensialitet: Prinsipp om at personopplysninger må være sikret mot at uvedkommende får tilgang til dem.

Lagringsbegrensning: Prinsippet om lagringsbegrensning innebærer at personopplysninger skal lagres slik at de slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.

Personvernkonsekvens: En følge som en beslutning eller endring får for personvernet.

Personopplysninger: Opplysning eller vurdering som kan knyttes til en enkeltperson. Dette kan f.eks. være:

14. navn, alder og fødselsnummer
15. adresse
16. telefonnummer og e-postadresse
17. opplysninger om elevenes underveis- og sluttevalueringer
18. fravær og anmerkninger
19. faglig progresjon



20. spesielle undervisningsbehov
21. atferdsmønstre og sosiale evner
22. kommunikasjon mellom elever
23. kommunikasjon mellom lærer og elev
24. informasjon om allergier
25. logg fra elevenes bruk av skolens nettverk
26. bilder, videoer eller lydfiler av elever

Sensitive personopplysninger (særlige kategorier): I loven er det definert en rekke kategorier av opplysninger som det skal mer til å kunne behandle enn andre opplysninger (artikkel 9 og 10 i forordningen):

13. Opplysninger om rasemessig eller etnisk opprinnelse.
14. Opplysninger om politisk oppfatning.
15. Opplysninger om religion.
16. Opplysninger om filosofisk overbevisning.
17. Opplysninger om fagforeningsmedlemskap.
18. Genetiske opplysninger.
19. Biometriske opplysninger med det formål å entydig identifisere noen.
20. Helseopplysninger.
21. Opplysninger om seksuelle forhold.
22. Opplysninger om seksuell legning.
23. Opplysninger om straffedommer.
24. Opplysninger om lovovertridelser.

Samtykke: En frivillig, spesifikk, informert, utvetydig og aktiv erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv. Et samtykke kan trekkes tilbake når som helst uten negative konsekvenser. Virksomheter må kunne dokumentere at samtykke er gitt.

Systemansvarlig: Operativt ansvarlig for de oppgaver systemeier har ansvaret for.

Systembruker: Alle som er tildelt rettigheter i det gjeldende IKT-systemet.

Systemeier: En systemeier er en leder som er ansvarlig for å utvikle, forvalte og drifte et informasjonssystem.