

Læreres mening om behandling av elevers personopplysninger i Google Workspace for Education

Oppsummering basert på intervjuer med lærere fra FUG

Innholdsfortegnelse

Introduksjon	3
<i>Kravet til å innhente den registrertes mening i GDPR</i>	3
<i>Lærere som registrerte</i>	3
Noen innledende merknader	3
Oppsummering av personvernbehandlingene	4
Vedlegg 1: Metode for innhenting av den registrertes mening	6
Vedlegg 2: Detaljert oppsummering av temaer	8

Introduksjon

Kravet til å innhente den registrertes mening i GDPR

Når du skal gjøre en personvernkonsekvensvurdering eller en DIPA (Data Protection Impact Assessment), er det et krav i GDPR artikkel 35 nr. 9 at du skal «innhente synspunktene på den planlagte behandlingen fra de registrerte eller den registrertes representanter».

Bestemmelsen understreker at du skal innhente den registrertes mening dersom det er «relevant».

Artikkel 29-gruppen¹ har i sin veileder på DPIA,² uttalt følgende:

The controller should also document its justification for not seeking the views of the data subjects, if it decides that this is not appropriate, for example if doing so would compromise the confidentiality of the companies' business plans, or would be disproportionate or impracticable.

Det betyr at det skal en del til før du kan *unnlate* å innhente den registrertes mening.

Lærere som registrerte

I forbindelse med det nasjonale DPIA- prosjektet for bruk av Google Workspaces for Education i skolen, så vi det som relevant å innhente meningen til lærere som registrerte om behandlingen av personopplysninger i Google Workspace for Education.

De personopplysningene som i all hovedsak behandles i Google Workspace for Education er personopplysningene til elever, som i kraft av å være barn er en sårbar gruppe i GDPRs forstand noe som betyr at behandling av deres personopplysninger bør gis et særlig vern.³ Elever kan ikke velge bort bruken av Google Workspace for Education alle tilsvarende verktøy som skoleeier har bestemt at skal brukes for å oppfylle forpliktelsene i opplæringsloven.

Personopplysningene til lærere som ansatte i kommunen behandles også i systemer som Google Workspace for Education. Lærer som ansatte kan heller ikke velge bort bruken av denne typen verktøy. I kraft av arbeidsavtalen er lærere tvert imot pålagt å bruke løsninger som Google Workspace for Education for å oppfylle sin del av arbeidskontrakten. Dette betyr at skoleeier har et særskilt ansvar for at også læreres personvern ivaretas ved bruken av løsninger som Google Workspace for Education.

Noen innledende merknader

Denne rapporten inneholder ikke alle de tingene som lærere var fornøyd med. Som det fremgår av metodebeskrivelsen i vedlegg 1, var formålet med å innhente den registrertes mening i forbindelse med denne DPIAen, å kartlegge personvernbeymringer. De positive sidene ved hvordan skoleeiers etterlever personvern, er derfor ikke tatt med i denne rapporten. I denne oppsummeringen har vi gjengitt de personvernbeymringene som vi mener er relevante for bruk av Google Workspace for Education. For en mer fullstendig oversikt over lærernes personvernbeymringer og tilbakemeldinger, se vedlegg 2.

¹ Nå det europeiske personvernrådet – The European Data Protection Board (EDPB)

² Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, adopted by Article 29 Data Protection Working Party on 4 April 2017

³ GDPR fortalepunkt 38

Oppsummering av personvernbehandlingene

Lærernes personvernbehandlinger kan oppsummeres slik:

1. Kontroll over lagring og sletting av elevdata

Flere lærere oppgir at det mangler klare retningslinjer for lagring, deling og sletting av data, noe som skaper usikkerhet rundt konfidensialitet og sikkerhet.

Langtidslagring av elevdata uten automatiserte slettesystemer øker risikoen for personvernbrudd. Lærerne etterlyser kortere lagringstider og bedre rutiner for håndtering av personopplysninger.

Særlig ser lærerne behovet for klare rutiner for lagring og sletting av elevdata etter endt skolegang.

2. Digital undervisning og læreres personvern

Bruk av private enheter for å få tilgang til skoleverktøy fører til en sammenblanding av privat og profesjonell informasjon, noe som kan utfordre lærerens personvern og resultere i utilsiktet deling av personopplysninger.

3. Behov for felles retningslinjer og opplæring

Manglende standardiserte retningslinjer og ulik praksis mellom kommuner når det gjelder bruk av Google Workspace for Education skaper forvirring. Mangel på opplæring og støtte i digitale verktøy fører til inkonsistent og usikker bruk av systemene.

Lærerne etterlyser en sentral instans som kan gi klare veiledninger om hvilke verktøy som er «GDPR-compliant» og egnet for bruk i skolen.

4. Tilgangsstyring og konfidensialitet

Flere lærere er bekymret over manglende oversikt over hvem som har tilgang til sensitive elevopplysninger. Lærerne etterlyser bedre kontroll over tilgangsnivåer for å sikre at sensitive data kun er tilgjengelige for de som trenger det.

5. Elevenes bruk av kommunikasjonsverktøy

Kommunikasjonsverktøy som Google Chat gir elever mulighet til å dele sensitive opplysninger med hverandre. Dette øker risikoen for spredning av personopplysninger og upassende innhold eller mobbing. Lærerne er bekymret for elevenes personvern og sikkerhet ved bruk av slike verktøy når bruken skjer uten tilstrekkelig kontroll.

6. Dataminimering og overvåkning

Lærerne er bekymret for omfattende logging og overvåkning av elevenes aktivitet i digitale verktøy, inkludert funksjoner som registrerer bruksdata og adferd. De påpeker behovet for å begrense innsamling av personopplysninger til det som er nødvendig, for å bevare skillet mellom skole og privatliv.

7. Reklame, datainnsamling og sporing

Bruk av tilleggstenester som YouTube og Google Søk eksponerer elever for reklame og uønsket datainnsamling. Lærerne er bekymret for at elever spores og utsettes for persontilpasset reklame, noe som bryter med prinsippet om et reklamefritt læringsmiljø og utfordrer elevenes personvern.

8. Bruk av bilder og samtykke

Lærerne opplever utfordringer med å sikre at bruk av bilder skjer i tråd med foreldre og elevers ønsker, og er bekymret for hvor og hvordan disse bildene lagres og slettes.

9. Utfordringer med flere digitale plattformer

Lærere uttrykker at bruk av både Google Workspace for Education og Microsoft 365 i samme kommune skaper forvirring, ineffektivitet og dobbeltarbeid. Det er bekymring for økt risiko for sikkerhetsbrudd, da informasjon spres over flere systemer uten enhetlig kontroll.

Vedlegg 1: Metode for innhenting av den registrertes mening

Identifisering av de registrerte

De registrerte ble representert av følgende organisasjoner:

1. Elevorganisasjonen

I denne DPIAen, er de registrerte først og fremst elever. Det var derfor viktig å enten intervju elever, eller finne en organisasjon som representerte elevene. Elevorganisasjonen ble kontaktet. Det viste seg at det ikke lot seg gjøre å samle et representativt utvalg elever for intervju, så elevene er representert ved et intervju av lederen av Elevorganisasjonen.

2. Foreldreutvalget for grunnopplæringa (FUG)

Særlig for yngre elever, er deres representant foresatte. Det nasjonale DPIA-prosjektet ønsket derfor også å innhente foresattes mening om behandling av barns personopplysninger i Google Workspace for Education. Det nasjonale DPIA-prosjektet tok kontakt med Foreldreutvalget for grunnopplæringa (FUG) som representant for foreldre til barn i skolen.

FUG tok så kontakt med sine medlemmer og fant foresatte som var interessert i å la seg intervju av prosjektet.

Ikke alle foresatte hadde barn som brukte Google Workspace for Education, men i de tilfellene brukte de sammenlignbare digitale verktøy.

3. Utdanningsforbundet

Lærernes personopplysninger behandles også i løsninger som Google Workspace for Education. Lærere som gruppe kan sammenlignes med elever i den forstand at de ikke har mulighet til å velge bort Google Workspace for Education når de er ansatt i en kommune hvor skoleeier tar i bruk dette verktøyet.

Det nasjonale DPIA-prosjektet tok kontakt med Utdanningsforbundet som så gikk ut til sine medlemmer og fant en gruppe lærere som ønsket å la seg intervju. I tillegg intervjuet prosjektet noen lærere fra de kommunene som har vært med i prosjektet.

Forberedelse og gjennomføring av intervjuer

I dette prosjektet ble det gjennomført intervjuer med hver enkelt informant. Hvert intervju tok ca 1,5 timer. Før intervjuet med den enkelte, sendte prosjektet en skriftlig beskrivelse av hvordan personopplysninger behandles. Denne informasjonen tilsvarer den delen av DPIA-en som beskriver behandlingsaktivitetene, og tok for seg både kjernetjenestene, tilleggstjenestene og Chrome-tjenestene i Google Workspace for Education. Dette var informasjon som også ble gjennomgått under intervjuet.

Deretter ble den registrerte stilt følgende spørsmål:

- 1. Basert på den informasjonen du har fått om hvordan personopplysninger behandles i Google Workspace for Education, hvilke personvernbeymringer har du?*

Formålet med dette spørsmålet var å identifisere mulige personvernrisikoer fra den registrertes perspektiv.

- 2. Hva ønsker du at skoleeier skal gjøre for å adressere disse beymringene?*

Med dette spørsmålet ønsket prosjektet å se om den registrerte hadde noen forslag til risikoreduserende tiltak som vi kunne bruke i DPIAen.

Den enkelte hadde også fått disse spørsmålene tilsendt på forhånd.

Referat fra intervjuet

Etter intervjuet ble det utarbeidet et skriftlig referat. Dette referatet ble sendt til den enkelte for verifisering slik at eventuelle feil kunne rettes. Dette for å sikre at de registrertes synspunkter ble nøyaktig gjengitt.

Utarbeidelse av rapport

Alle intervjuene ble så lest gjennom og informasjonen ble sammenstilt i denne rapporten.

Vedlegg 2: Detaljert oppsummering av temaer

Kapittel 1: Kontroll på lagring av elevdata

1.1 Sikker deling

Bruken av delte disker for ansatte, som ikke kan integreres med Google Classroom, skaper utfordringer. Sensitive dokumenter som elevvurderinger lagres her, og det er uklart hvem som har tilgang til disse filene, noe som skaper usikkerhet knyttet til konfidensialitet og sikkerhet i løsningen.

Noen av lærerne vi intervjuet oppgir at elever, selv de yngste, kan dele materiale og kommunisere fritt på tvers av enhetene, noe som har ført til bekymringer blant både lærere og foreldre. Funksjoner som tillater elevene å dele lydfiler og annet innhold har vært kontroversielle, og foreldre uttrykker skepsis til hvor data lagres og hvem som har tilgang. Når elever laster ned dokumenter etter endt skolegang, kan disse inkludere samskrivingsdokumenter med bidrag fra medelever, og det er usikkert om alle har samtykket til at deres bidrag deles videre. Lærerne opplever dette som et mulig brudd på personvernet.

Lærerne er også usikre på om data slettes ordentlig fra Google Workspace for Education. De etterlyser klarere retningslinjer for hvordan data lagres, deles og generelt brukes, og understreker behovet for sikker og tydelig datalagring som ivaretar elevenes personvern.

Selv om kommunen har tatt grep for å begrense data som lagres i digitale møter og har stengt grupper med uønsket adferd, føler lærerne at det fortsatt mangler kontroll over hvilke data som tas ut og lagres.

1.2 Lagring og sletting

Oppbevaring av elevdata over lengre tid har skapt bekymring blant lærerne. Data som elevarbeid og skjemaer fra tidligere skoleår er fortsatt tilgjengelige mange år senere, noe som kan utgjøre en risiko for elevenes personvern. Behovet for kortere lagringstid og bedre rutiner for lagring av personopplysninger blir derfor fremhevet som viktig. Noen lærer oppgir at det ikke finnes automatiserte prosesser for sletting etter tre år, noe som skaper usikkerhet rundt hva som lagres og hvem som har tilgang til eldre data.

Selv om kommunen jobber systematisk med informasjonssikkerhet og personvern, opplever lærerne at det mangler klare rutiner for å håndtere og slette dokumenter om elevsamtaler og andre data som samles inn i løpet av skoleåret. Selv om retningslinjer eksisterer, oppleves praksisen på feltet som mangelfull, noe som ytterligere forsterker bekymringen rundt lagring og sletting av særlig sensitive personopplysninger.

1.3 Åndsverk

Det er ikke alle kommuner som har åpnet for bruk av Google Takeout.⁴ Fraværet av Google Takeout gjør det vanskelig for elever å laste ned sine egne data ved avslutning av skoleåret. Dette begrenser deres kontroll over eget åndsverk, noe læreren ser som en ulempe både for personvern og praktisk bruk.

⁴ Funksjonalitet som gjør det mulig for elever å laste ned dokumenter fra skolekontoen sin til en privat Google-konto

Hos andre kommuner tar elevene med seg alle dataene sine når de forlater skolen. Dette inkluderer også samskrivingsdokumenter og annen informasjon om medelever. Dette kan utgjøre en potensiell personvernrisiko, da ikke alle medelever nødvendigvis har gitt samtykke til at deres bidrag deles videre. Det samme gjelder for lærere som bytter jobb og tar med seg data som kan inneholde sensitive opplysninger eller åndsverk tilhørende andre.

De lærerne som arbeider i kommuner som har et system for at elever kan ta med seg eget elevarbeid, er tilfredse med at elever kan ta med sine vurderinger fra Google Classroom når de forlater skolen, men ser behovet for at disse dataene slettes etter endt skolegang for å beskytte både elevenes og lærernes åndsverk. Mangelen på klare rutiner for lagring og sletting av elevdata reiser spørsmål om hvordan åndsverk og personopplysninger håndteres. Noen lærere etterlyser behovet for bedre rutiner for hvordan personopplysninger behandles, lagres og slettes.

Kapittel 2: Digitale plattformer påvirker læreres privatliv og personvern

Lærere opplever at de i digitalundervisning må være synlige på kamera, mens elevene kan velge å være anonyme. Dette er en ubalanse som påvirker lærerens personvern, særlig når undervisningen skjer i lærerens eget hjemmemiljø.

Noen lærere fremhever at de kan bruke mobiltelefoner og andre private enheter for å få logge seg på Google Workspace for Education og på den måten så tilgang til elevenes personopplysninger. Dette skaper uklarhet mellom jobb- og privatbruk og kan føre til utilsiktet deling av personlig informasjon.

Det er også utfordringer knyttet til sammenkobling av private og profesjonelle roller, spesielt når læreren kobler seg til Google Workspace for Education via hjemmenettverket. Dette øker risikoen for en sammenblanding av lærerrollen. Videre må lærere ofte bruke skoleverktøy og apper på private enheter, noe som reiser spørsmål om kontroll og personvern. Kravet om å installere visse apper som Transponder blander privat og profesjonell informasjon og skaper usikkerhet rundt beskyttelsen av disse personopplysningene.

Kapittel 3: Behov for felles retningslinjer, tydeligere styring og klarere informasjon

Noen kommuner har innført strenge begrensninger, men forskjeller i tillatelser mellom ulike kommuner skaper forvirring blant lærerne. Dette understreker behovet for en sentral instans som kan standardisere vurderingene og gi klare retningslinjer for hvilke tjenester som er «GDPR-compliant» og egnet for bruk i skolen.

Læreren har opplevd at kommunen har gitt feilaktige instruksjoner om personvernregler, noe som har resultert i kritiske spørsmål fra informerte foreldre. Dette understreker behovet for sentrale føringer som kan gi tydelig veiledning og oppdatere skolen om endringer i systemene for å ivareta personvernet bedre.

Mangelen på støtte og opplæring i digitale verktøy forverrer situasjonen. Noen av lærerne vi intervjuet har fått minimal opplæring i bruk av Google Workspace av kommunen, og det finnes lite kontinuerlig støtte for lærere som skal bruke verktøyene i undervisningen. Dette har ført til at lærere bruker verktøyene på ulike måter, noe som gjør det utfordrende å sikre konsistent og trygg bruk av systemene.

Videre gjør kommunen beslutninger rundt GDPR som påvirker arbeidsflyten, men disse valgene implementeres ofte uten forvarsel, noe som skaper praktiske utfordringer. Eksempler inkluderer endringer i tilgjengelige funksjoner i Google Docs og at arbeidsplaner nå må sendes som PDF-er.

Noen lærere oppgir at det tidligere var omfattende bruk av gratisprogrammer. Imidlertid håper lærerne på mindre bruk av dette takket være en tydeligere bevisstgjøring og strammere regler i kommunen. Bruken av slike verktøy innebærer økt risiko for personopplysninger som samles inn utenfor kommunens systemer. Alt dette peker mot et sterkt behov for felles retningslinjer, tydeligere styring og klarere informasjon for å sikre at personvernet ivaretas og at lærerne kan utføre sitt arbeid effektivt.

Kapittel 4: Tilgangsstyring

Noen av lærerne er bekymret for manglende oversikt over hvem som har tilgang til sensitive elevopplysninger. Elever rapporterer ofte mobbing eller vold muntlig, noe som så dokumenteres skriftlig, men det er uklart hvem som har innsyn i denne typen personopplysninger. Dette skaper usikkerhet rundt håndteringen av personopplysninger om elever med særskilte behov eller beskyttelsesbehov.

Noen av lærerne uttrykker behov for gode lagringsystemer som gjør det mulig å notere og lagre opplysninger om elevene på en trygg måte. Selv om tilgangen til informasjon i Google Classroom er ryddig strukturert, etterspør noen av lærerne klarere kontroll over hvem som har tilgang og hvor mange lagringsplasser som eksisterer. Mangelen på oversikt over tilgangsnivåer gjør det vanskelig å sikre at sensitive data kun er tilgjengelige for de som trenger det.

Videre krever Google Classroom at vikaransvarlige legges til i klasserommet, noe som kan føre til at personopplysninger om elev som bare skal være tilgjengelig for hovedlæreren, blir tilgjengelige for andre. Lærere opplever dette som et brudd på elevens personvern og prøver å unngå det ved å bruke skjermdumper i stedet. Dette understreker behovet for bedre tilgangsstyring for å forhindre konfidensialitetsbrudd og utilsiktet deling av sensitive personopplysninger.

Kapittel 5: Kommunikasjonsverktøy

5.1 Elevenes bruk av Chat-funksjoner

Noen lærere oppgir at i deres kommune bruker elever Google Chat uten tilsyn, noe som har skapt bekymringer rundt deling av personopplysninger. De kan dele sensitive opplysninger om seg selv og andre uten å tenke seg om, noe som kan føre til at personopplysninger spres.

Chatten brukes også utenfor skoletid, og mangelen på en funksjon for automatisk sletting av meldinger etter en gitt periode øker risikoen for at uønsket informasjon forblir tilgjengelig. Selv om skolebaserte meldingssystemer anses som sikre, er det alltid en risiko for konfidensialitetsbrudd. Logger over endringer i delte dokumenter kan inneholde upassende innhold fra elever, noe som potensielt kan påvirke dem senere.

Flere lærere trekker frem at under covid-19 var chat-funksjonen spesielt nyttig for å opprettholde kommunikasjonen mellom lærer og elev. Nå er funksjonaliteten fortsatt tilgjengelig selv om nytteverdien og bruken er begrenset. Noen lærere uttrykker bekymring for om elevene på barneskolen i det hele tatt bør ha tilgang til egne kommunikasjonskanaler uten foreldreinnsyn, spesielt siden chat brukes lite i undervisningen på dette nivået. Det etterlyses mer bevissthet fra kommunens side om hvilke verktøy skolen egentlig har bruk for.

Bruken av videofunksjoner som Google Meet har også reist spørsmål. Under pandemien kunne elever invitere medelever utenfra eller til og med fra andre skoler, og det var en utfordring at eleven som logget på først, fikk rollen som leder i samtalen.

5.2 Kommunikasjon med foresatte

Noen lærere understreker at kommunikasjon med foreldre skal skje gjennom sikre systemer som Visma. Imidlertid foretrekker foreldre ofte å kommunisere direkte med lærer via e-post, som kan føre til at personopplysninger (også sensitive personopplysninger) behandles utenfor de etablerte systemene. Noen lærere etterlyser bedre løsninger og verktøy for å forenkle kommunikasjon og sikre at personopplysninger behandles sikkert og i henhold til kommunens retningslinjer.

Kapittel 6: Dataminimering

Noen av lærerne vi har intervjuet er bekymret for at samskriving i dokumenter gir elever mulighet til å dele hva de vil, noe som kan føre til at de utleverer seg selv på måter de kanskje ikke burde, eller til å skrive sårende ting om andre. Selv om elever stort sett forstår at dokumenter som lages i Google Classroom kan leses av læreren, ser lærere behov for begrensninger i hva som deles for å beskytte elevenes personvern.

Google Workspace logger også når elever og lærere bruker verktøyene, noe flere lærere mener er unødvendig detaljert. Dette spesielt når det ikke er klart hvilke personopplysninger som logges. Flere lærere påpeker at det må være grenser for hvilken informasjon som samles inn, for å bevare skillet mellom skole og hjem.

Noen lærere påpeker at elever må opprette brukerkontoer på Google Workspace for å kunne delta i skolen, noe som betyr at skoleeier må være ekstra påpasselig med å ivareta elevenes personvern. Spesielt må skoleeier være bevisst på at elevene ikke skal bruke løsninger som sporer dem unødvendig eller hvor det innhentes flere personopplysninger enn det som er nødvendig. I tilleggstjenestene kan Google f.eks også samle informasjon om applikasjoner, nettlesere og enheter som elever bruker, inkludert mobilnummer og lokasjonsdata, noe lærere finner problematisk.

Selv om kommunen har sikret seg Google Workspace med klare rammer, skapes det store mengder personopplysninger i løsningen når elever produserer innhold og generelt interagerer med de forskjellige Google-tjenestene (aktivitetsdata). Disse personopplysningene må også håndteres sikkert.

Funksjoner som Google Meet Attendance List og Draftback gir læreren mulighet til å overvåke elevenes aktivitet, noe som har sine fordeler, men reiser også bekymringer knyttet til elevenes personvern og hvor mye informasjon som lagres om deres digitale adferd.

Kapittel 7: Konfidensialitetsbrudd

Selv om hybridundervisning brukes minimalt, uttrykker noen lærere bekymring for muligheten for uønsket tilstedeværelse under slike økter. Felles kode for pålogging på digitale tavler gir alle elever tilgang til samme system, noe som potensielt gir dem mulighet til å bruke tavlen uten lærerens viten. Lærere opplever også begrenset funksjonalitet i å lagre og dele informasjon fra tavlen til elever, noe som kan føre til at sensitiv informasjon ikke håndteres forsvarlig.

På Chromebooks kan elever logge inn på ulike enheter, noe som gjør det utfordrende å sikre konfidensialitet og sikkerhet. Dette gir elevene frihet til å dele og streamme innhold. En av lærerne vi intervjuet hadde opplevd et tilfelle der en elev filmet en hel time. Læreren ser dette som en risiko for at personopplysninger kommer på avveie, spesielt for elever med beskyttelsesbehov.

Kapittel 8: AI

Noen lærere tok på eget initiativ opp personvernbeholdninger knyttet til bruk av AI i skolen. De trakk frem risikoer som at AI kan plukke opp sensitiv informasjon om elever, noe som kan ha negative konsekvenser for dem senere i livet, for eksempel i forsikringsaker eller andre typer viktige avgjørelser.

Kapittel 9: Bekymringer knyttet til tilleggstjenester i Google Workspace for Education

9.1 Reklame, datainnsamling og sporing

Flere lærere trekker frem at de synes forbudet mot reklame i skolen utfordres ved bruk av digitale verktøy. Elevene eksponeres for reklame når de forlater de reklamefrie læringsverktøyene (f.eks. YouTube og Google søk), noe lærere ser som en åpenbar utfordring. Til tross for løfter om reklamefrie opplevelser, blir elever utsatt for annonser på f.eks. YouTube. Flere lærere uttrykker også bekymring for at elevene spores og eksponeres for adferdspasert og persontilpasset reklame. Noen lærere mener den reklamen elever utsettes for på YouTube tilpasses deres bruk og aktivitet, noe som bryter med prinsippet om et reklamefritt læringsmiljø.

Noen lærere oppgir at bruk av Google Maps og funksjonalitet knyttet til lokasjonsdata har blitt deaktivert i den kommunen de jobber for. Likevel er disse lærerne usikre på om elevene forstår mengden informasjon de legger igjen i denne typen tjenester. Mange elever søker på engelsk, noe som kan gi Google mer innsikt i deres språkpreferanser og vaner. Bekymringen strekker seg også til YouTube og andre nettsider med reklame som kan samle inn personopplysninger om elever. Lærerne uttrykker bekymring over elevenes manglende forståelse for datainnsamling gjennom søk og reklame.

En måte å bruke YouTube på som begrenser Googles innsamling av personopplysninger om elever, er at læreren lenker til YouTube-videoen og deler den med elevene i Google Classroom. Selv om lenking til YouTube i undervisningen brukes for å unngå reklame, er det uvisst hvilken data som samles inn fra elevene. Google samler informasjon om elevene gjennom tjenester som YouTube, noe læreren mener er unødvendig og potensielt et brudd på elevenes personvern.

9.2 Innholdsbegrensning

Flere lærere ser behovet for bedre kontroll og begrensninger på nettressurser som YouTube. Det at læreren deler videoer via lenker i Google Classroom, reduserer risikoen for at elevene blir utsatt for et bredt spekter av innhold uten effektiv alders- eller innholdskontroll. Denne typen begrensninger er viktige for å beskytte særlig de yngste elevene. Det nevnes at lærere må være bevisste på hvilken type innhold de tar i bruk i undervisningen.

Noen lærere ønsker seg en reklamefri versjon av YouTube.

Kapittel 10: Bruk av bilder av elever i skolen

Noen lærer mener det er ikke alltid er klart om elevene har samtykket til at profilbilder av dem brukes. Profilbilder kan ses av mange, noe som kan eksponere elevene på en måte som bryter med deres personvern. Dette er særlig problematisk for de elevene som ikke har fått foreldresamtykke til bruk av profilbilder.

Noen lærere oppgir at de jobber i kommuner som har begrenset bruken av profilbilder. Tidligere kunne elever bruke egne profilbilder, men lærerne oppgir at dette har blitt begrenset etter uheldige episoder.

Flere læreren opplever utfordringer med samtykke til bruk av bilder og identifisering gjennom e-post og andre kommunikasjonssystemer. Det oppleves som vanskelig å ivareta elevenes personvern med tanke på bruk av profilbilder spesielt når foreldre og elever selv ikke følger retningslinjene. Noen lærer uttrykker også bekymring rundt hvor disse bildene lagres, og hvorvidt de noensinne slettes.

Kapittel 11: Utfordringer med bruk av flere digitale plattformer

Noen lærere oppgir at de jobber i kommuner hvor oppvekst bruker Google Workspace for Education, mens resten av de ansatte i kommunen bruker Microsoft 365. Dette gjør administrasjon og støtte mer utfordrende og kan skape flere sikkerhetsrisikoer. Noen lærere må bruke både Google Workspace og kommunens Microsoft-system, og det skaper forvirring og ineffektivitet. Spesielt innen kommunikasjon må de navigere mellom Gmail og Outlook, samt Teams og Google Meet. Denne konflikten mellom plattformer fører til dobbeltarbeid og øker risikoen for sikkerhetsbrudd, da informasjon spres over flere systemer uten enhetlig kontroll.