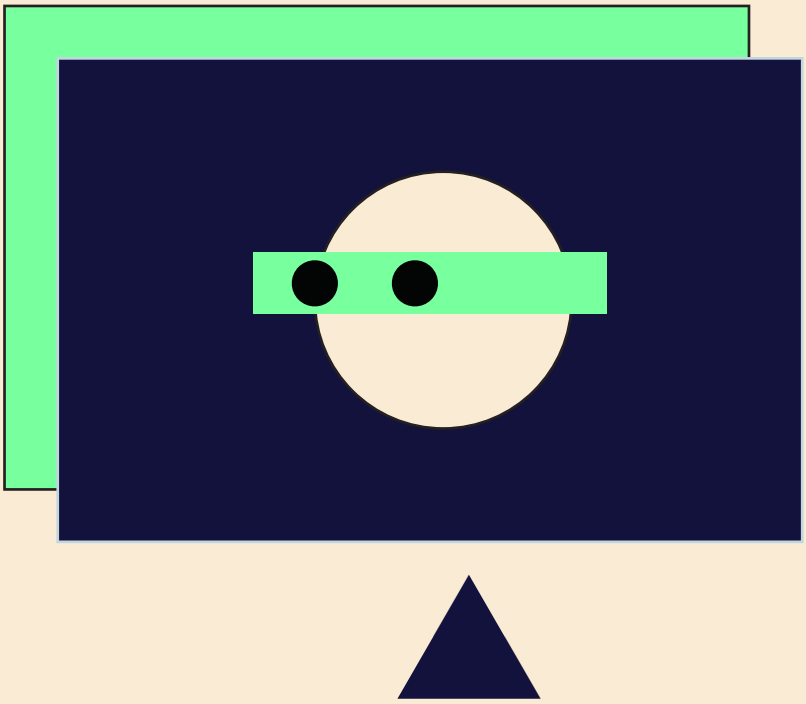
bouvet



RAPPORT

Digitalisering i skolen

# Har vi glemt personvernet?

## Skrevet av:

Åsmund Mæhle
Birgitte Fjærestad
Torkil Grimsrud
Martin Gravråk
Simen Sommerfeldt

bouvet.no

**2021**

# Innhold

# Sammendrag

Skolen ble heldigital over natten 12. mars 2020. Svært mange elever, lærere, skoleledere og skoleeiere ble stilt ovenfor en helt ny situasjon der personvernet ikke alltid fikk første prioritet. På samme tid begynte Datatilsynet å skrive ut bøter til kommuner som ikke overholdt personvernet i skolen.

I Bouvet er vi opptatt av en god og trygg skole der elevenes lovfestede personvern blir ivaretatt. Derfor har vi foretatt en undersøkelse av hvordan det står til med elevenes personvern. I undersøkelsen ser vi på et bredt spekter av situasjoner i skolen der personvern er utfordrende. Dataene er hentet inn gjennom dybdeintervjuer med lærere, skoleledere og skoleeiere i sju kommuner. Vi har også snakket med viktige aktører i sektoren så som KS, IKT Norge og Datatilsynet. I tillegg har vi sett nærmere på noen av de gratis læringsressursene som lærere har tipset hverandre om under korona.

### Her er hva vi fant ut:

- Bruk av gratisverktøy innebærer en stor risiko for at informasjon om elevene kommer på avveie.
- Elever får ikke så gode læringsverktøy som de kunne fått. Dette er særlig et problem i mindre kommuner. Det er fordi hver eneste kommune må gjøre risikoanalyser og skrive databehandleravtaler for hvert verktøy, noe som er svært ressurskrevende.
- Elevenes e-postadresser kan brukes til svindelforsøk.
- Ansatte i skolen kjenner ikke rutinene for hva som skal gjøres dersom informasjon om elevene kommer på avveie.
- Håndtering av sensitive personopplysninger er tungvint og gjør at ansatte tar i bruk sårbare skyggesystemer.
- Innføring og bruk av læringsplattformer og skoleadministrative systemer har blitt bedre med hensyn til personvern, men innebærer fortsatt personvernrisiko dersom ansatte bruker verktøyene feil.
- Å få foreldrene til å bruke trygge applikasjoner for dialog med skolen er vanskelig.
- Det hjelper ikke om systemene i seg selv er sikre dersom de brukes feil eller personinformasjon legges i feil system. Kompetansen og bevisstheten blant ansatte om trygg håndtering av personinformasjon er svært varierende.

### Våre anbefalinger: Hva bør skje nå?

I denne rapporten peker vi på at skoleeiere og lærere står i en skvis mellom det å gi en best mulig opplæring og samtidig ivareta elevenes personvern.

Vi mener følgende tiltak må til for å sikre personvernet, gi bedre opplæring og utnytte de digitale læringsressursene bedre:

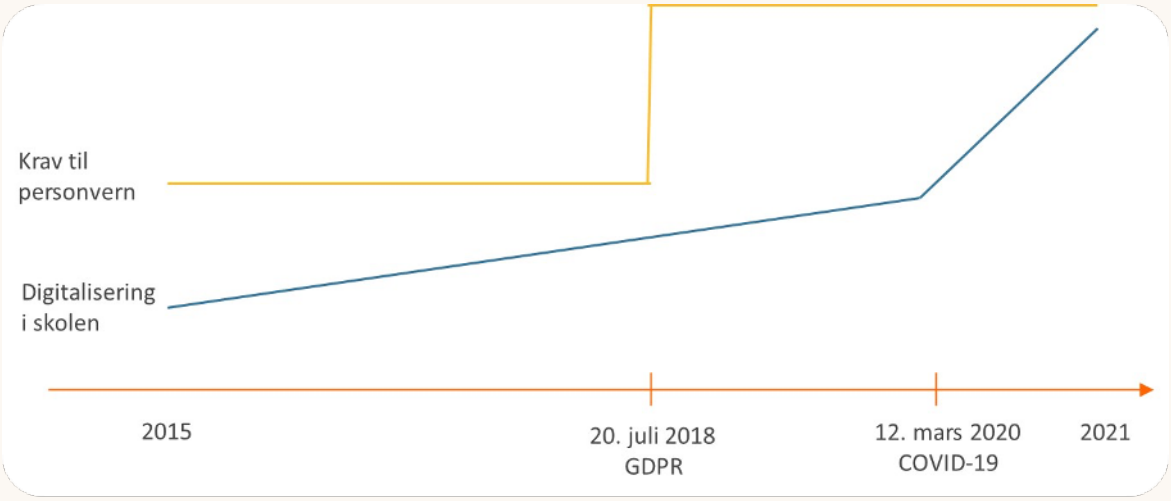
- Hver kommune kan ikke sitte med hele oppgaven med å vurdere ulike verktøy i hvert av de 15 fagene i 10 årstrinn. Arbeidet med risikoanalyser og databehandleravtaler for digitale verktøy må samordnes og effektiviseres. Dette kan gjøres ved å realisere en felles tjenestekatalog for digitale læringsressurser som regjeringen har foreslått i sin handlingsplan for digitalisering av grunnopplæringen[1]. Gjennom en slik katalog vil elever og lærere i distriktene få tilgang til bedre verktøy. Et slik grep vil også bidra til at verktøy som er for dårlig på personvern holdes utenfor norsk skole.
- Norsk skole trenger tydelige kjøreregler som forklarer hvorfor personvern er viktig og hvordan det skal ivaretas. Kompetansen og bevissthet om digitalt personvern hos lærere, skoleledere og skoleeiere må bygges systematisk.
- Systemer og rutiner for håndtering av sensitiv informasjon om elevene internt i skolesystemet og på tvers i kommunen må på plass. Forslag til verktøy og rutiner som trygger de situasjonene vi gjennomgår i rapporten, bør utvikles sentralt slik at den enkelte lærer og skole slipper å ta utrygge valg.
- KS er en organisasjon som kjenner skoleeiernes hverdag godt. En styrking av KS sin satsing på Skolesec vil derfor være et godt tiltak for å møte de utfordringene skolen står ovenfor når det gjelder personvern.

Vi oppfordrer Utdanningsdirektoratet og Kunnskapsdepartementet til å komme på banen for å iverksette grepene som nevnt over **så fort som mulig.**

1 https://www.regjeringen.no/contentassets/44b8b3234a124bb28f0a5a22e2ac197a/handlingsplan-for-digitalisering-i-grunnopplaringen-2020-2021.pdf

# 1. Innledning

12. mars 2020 stengte alle norske skoler ned. Det førte til en eksplosjon i digitaliseringen. All undervisning, all dialog og all administrasjon måtte nå gjøres digitalt. Mindre enn to år tidligere trådte den nye personopplysningsloven i kraft. Den setter detaljerte krav til behandlingsansvarlig når det gjelder formål og rutiner og gir nye rettigheter til innbyggerne. Dette var utgangspunktet for at vi i Bouvet ønsket å se på hvordan det har gått med personvernet i skolen under korona-pandemien.




Bouvet har som visjon å gå foran og bygge fremtidens samfunn. Det innebærer også at vi ønsker å bidra til en bedre og sikrere skole. Gjennom denne rapporten ønsker vi å bidra til samfunnet ved å løfte temaet personvern i skolen enda høyere på dagsorden.

Det er andre som kan mer om skolen enn oss, og som kjenner situasjonen på kroppen hver eneste dag. I denne undersøkelsen har vi intervjuet noen av disse. Selv har vi i Bouvet jobbet med digitalisering i utdanningssektoren i 20 år og har i tillegg en solid kompetanse på personvern, informasjonssikkerhet og analysearbeid. Til sammen håper vi at denne rapporten kan gi et bilde av tilstanden.

Vi er dypt imponert over den innsatsen som lærere, skoleledere og skoleeiere har gjort i koronaperioden. De klarte i løpet av noen dager i mars 2020 å legge om arbeidsform, rutiner og verktøy helt. Senere har de måttet omstille seg på kort varsel en rekke ganger. Samtidig har de stått i første rekke og blitt eksponert for smittefare gjennom sitt møte med elevene.

# 2. Hvordan vi har samlet data

For å samle data til denne rapporten har vi gjennomført dybdeintervjuet og gjort analyser av gratis digitale verktøy som lærere har anbefalt til hverandre på nettet.

I intervjuene har vi snakket med lærere, representanter for skoleeiere og en rektor i til sammen sju kommuner av ulik størrelse. Intervjuene ble gjennomført av en sikkerhetsarkitekt og en rådgiver med erfaring fra utdanningssektoren.

I tillegg har vi hatt samtaler med Datatilsynet, Skolesec-prosjektet i KS og FIKS ved Det utdanningsvitenskapelige fakultet ved Universitetet i Oslo.

# 3. Digitalisering og personvern i skolen

> «Skolen har fått lov til å bruke teknologien på en spennende og innovativ måte i læringsøyemed. De kan fråtse i spennende teknologi og nyvinninger for å drive med en pedagogisk og fornuftig opplæring av elevene. Teknologien gir utrolige muligheter, men det er ikke enhver teknologi som er personvernvennlig. Digitaliseringen har gått utrolig fort. Det er vanskelig i det løpet der å henge med på kravene og detaljene som er i personregelverket i dag.»
>
> *Juridisk seniorrådgiver Charlotte Bayegan, Datatilsynet*
> *I Personvernodden fra Datatilsynet 4. mars 2021*

De siste to tiårene har det vært en sterk digitalisering av norsk skole. Det har oppstått behov for et stort antall applikasjoner knyttet til drift av skolene. Eksempler på dette er:

- Skoleadministrative systemer for å håndtere elever, klasser, timeplaner og karakterer
- Læringsplattformer for å tilgjengeliggjøre læringselementer og ta imot innleveringer fra elever
- Digitale læringsressurser i de ulike fagene
- Samhandlingsløsninger for deling av dokumenter
- Systemer for chat og videodialog
- E-postsystemer
- Systemer for dialog mellom hjem og skole
- Systemer for sikker samhandling med andre kommunale enheter

**Også en rekke av kommunenes felles systemer brukes av skolen:**

- Sak/arkiv-systemer
- Kvalitets- og avvikssystemer
- Personvernapplikasjoner for å holde orden på hvilke personopplysninger som behandles i hvilke systemer, med hvilket formål og behandlingsgrunnlag og om ROS-analyse og databehandleravtale finnes

Det lagres personopplysninger i mange av disse applikasjonene. Store og små kommuner og fylkeskommuner har ansvar for at personopplysninger behandles riktig av alle ansatte i hver av disse systemene. Det sier seg selv at dette er en stor og komplisert jobb.

*I flere hundre år fram til begynnelsen av 2000-tallet var det tavle, kritt, skolebøker, skrivebøker og blyanter som dominerte i klasserommet. Elevene leverte lekser på papir og fikk tilbakemelding på papir. Elevlister, karakterer og anmerkninger ble også ført på papir. Meldinger til hjemmet ble skrevet i meldingsboka eller kom med ranselpost. Så lenge lærerne passet på papirene sine og passet munnen sin, så var det få utfordringer knyttet til personvern.*

## 3.1 Ny personopplysningslov i 2018

Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger[2]. Det er tatt inn en egen paragraf om personvern i grunnloven. I tillegg er personvernet forankret i den europeiske menneskerettskonvensjonen.

Personopplysningsloven fra 2018 bygger på noen grunnleggende prinsipper[3]:

2 Kilde: https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/
3 Kilde: https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/

- Behandling av personopplysninger skal være lovlig, rettferdig og gjennomsiktig.
- Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål.
- Det skal ikke samles inn mer personopplysninger enn det som er nødvendig for formålet
- Personopplysninger som behandles skal være korrekte og oppdaterte.
- Personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendig.
- Personopplysninger skal behandles slik at opplysningenes integritet, konfidensialitet og tilgjengelighet beskyttes.
- Alle som behandler personopplysninger, er ansvarlig for å følge reglene for behandling.

Personvern var ikke noe nytt da GDPR og ny personopplysningslov kom i 2018. Den første personopplysningsloven fra 2000 (som erstattet personregisterloven fra 1978) satte klare krav til behandling av personopplysninger. Men den nye loven var langt mer detaljert med hensyn rettigheter til innsyn og sletting samt krav om rutiner, behandlingsgrunnlag og formål.

Etter 2018 har det vært en kraftig økning i antall bøter og irettesettelser Datatilsynet har gitt[4]:

| **År** | **Antall sentrale vedtak fra Datatilsynet** |
|---|---|
| 2021 | 20 (fram til juli) |
| 2020 | 11 |
| 2019 | 5 |
| 2018 | 0 |
| 2017 | 3 |
| 2016 | 1 |
| 2015 | 1 |

I 2019 skrev Datatilsynet ut de første gebyrene til skoleeiere for brudd på personopplysningsloven. Siden da har Datatilsynet gitt følgende gebyrer til ulike skoleeiere:

4 Kilde: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/ Besøkt 2. august 2021

- Gebyr på 1,2 millioner kroner for overtredelse av personopplysningssikkerheten i mobilapplikasjonen Skolemelding. (2019)
- Gebyr på 1,6 millioner kroner for mangelfull personopplysningssikkerhet i datasystemene brukt i grunnskolen. Brukernavn og passord for 35 000 bruker lå tilgjengelig for ansatte og elever. (2019)
- Gebyr på 3 millioner kroner for mangelfull sikring av personopplysninger i kommunikasjon mellom skole og hjem. (2020)
- Gebyr på 500 000,- kroner etter at helseopplysninger om barn ble behandlet i læringsplattformen Showbie. (2020)
- Gebyr på 50 000,- kroner til kommune for deres bruk av treningsapplikasjonen Strava i undervisningen. (2021)

I tillegg har tre kommuner fått irettesettelse av Datatilsynet for feil bruk av Googles løsninger i skolen. En annen kommune har fått pålegg om å avslutte bruken av en applikasjon for å kartlegge mobbing i skolen.

Disse gebyrene og irettesettelsene har hatt effekt. Kommunene som har fått gebyr, har gjort kraftige forbedringer av rutiner og systemer. Gebyrene har fått mye oppmerksomhet i media og er godt kjent i skole-Norge. Dette har bidratt til å løfte bevisstheten om personvern i skolen.

En spørreundersøkelse som Utdanningsdirektoratet har gjennomført, viser likevel at 30 prosent av skolene ikke har gode rutiner for registrering, bruk, lagring og sletting av persondata[5].

Ifølge KS er skolen blant de sektorene som har digitalisert raskest, men uten at det har fulgt med tilsvarende kompetanseutvikling eller kulturendring. Det har gitt skolene lavt omdømme når det gjelder personvern.

> «Jeg fikk panikk da jeg leste om kommunen som fikk gebyr for bruk av Strava»
>
> **Representant for skoleeier**

> «I 2018 med GDPR ble man svett. Da bøtene til skoleeiere begynte å komme ble man enda svettere.»
>
> **Christian Sørbye Larsen, Skolesec / KS**

5 https://www.regjeringen.no/no/aktuelt/vil-styrke-kommunenes-digitaliseringsarbeid-i-skolene/id2788319/

## 3.2 Nedstengningen i mars 2020

Det var svært varierende hvor langt de ulike kommunene hadde kommet den dagen statsministeren annonserte at alle skoler skulle stenges. Systemer for administrasjon av elever og klasser var på plass. De aller fleste skoleeiere hadde også læringsplattformer der lærere kunne legge ut materiell og elevene kunne gjøre innleveringer. Langt de fleste hadde også tatt i bruk digitale læremidler i større eller mindre grad. Ifølge en pressemelding fra Kunnskapsdepartementet fra desember 2020 er det 70 prosent av kommunene som har *en* digital enhet per elev[6].

**Digital undervisning og dialog:** Den store forskjellen som kom i mars 2020, var at alle skoletimer og all kommunikasjon mellom skole, lærer, elev og hjem måtte foregå digitalt. Lærere, skoleledere og skoleeiere vi har intervjuet, forteller at de måtte kaste seg rundt og få på plass rutiner og systemer for videoundervisning og chat. Det var høyst varierende hvor mye opplæring lærerne fikk i bruk av verktøyene.

I intervjuene har det kommet fram at skolene har opplevd episoder der chat mellom elever har utartet eller at elevene har skrevet stygge ting om hverandre. Dette ser likevel ut til å være et større problem i private kanaler utenom skolen. I skolens kanaler er alle pålogget under fullt navn og det er lett for skolen å avdekke hvem som har sagt hva.

En del kommuner etablerte rutiner for å ivareta personvernet i den digitale dialogen mellom lærer og elev. Eksempel på dette var:

- Lærere skulle ikke ha lyd fra elevene ut i rommet på hjemmekontoret.
- Elevene ble oppfordret til å bruke bakgrunnsbilde ved hjemmeskole.
- Det ble laget retningslinjer for bruk av chat. En kommune forteller om sperre for visse ord samt at skolens chat-kanal ble stengt i ferien for å forhindre mobbing.
- Noen kommuner sperret for at elevene kunne ta kontakt med hverandre på video.

**Digitale læremidler:** Med bare digital undervisning måtte alle lærere kaste seg rundt og tenke annerledes. Flere skoleeiere vi har intervjuet, forteller om et stort ønske fra lærerne om å få bruke både lisensierte og gratis læringsressurser på nettet. Facebook-gruppen *Koronadugnad for lærere* ble opprettet og fikk i løpet av noen dager 60 000 medlemmer. Ildsjeler jobbet dag og natt for å hjelpe andre lærere med tips om digital undervisning.

6 https://www.regjeringen.no/no/aktuelt/vil-styrke-kommunenes-digitaliseringsarbeid-i-skolene/id2788319/


*Eksempel på dialog mellom lærere på Facebook. Det var spesielt mye av dette i tiden rett etter 12. mars 2020.*

> «Da Covid kom var det mange som ønsket å bruke gratis læringsressurser. De tenkte så ut av boksen at de sprengte rammene.»
>
> **Representant for skoleeier**

**Stor fordel for kommuner som hadde kommet langt i digitaliseringen:** Intervjuene våre viser at kommuner som før mars 2020 hadde fått på plass nettbrett/PC til alle elever og hadde etablert løsninger for video og kommunikasjon, fikk en mye enklere start på koronatiden. Det var også enklere i de kommunene der lærerne hadde tilgang til skoleadministrative systemer fra hjemmekontoret.

> «Korona ble syretesten på digitaliseringsarbeidet vårt»
>
> **Representant for skoleeier**

**Korona ga et digitaliseringsløft med nytteverdi etter korona.** Flere lærere forteller i intervjuene om at skifte til digital undervisning var utfordrende, men at de har måttet lære seg mye om bruk av digitale verktøy som vil være nyttig senere.

**Personvernet kom i andre rekke i starten.** Vårt inntrykk fra datainnsamlingen er at det var undervisningen og ikke personvernet som kom i første rekke da skolene ble stengt ned i mars 2020. Skolene og lærerne måtte kaste seg rundt i full fart for å få den digitale opplæringen til i det hele tatt å virke. Regler og rutiner kom i større grad på plass etter hvert

## 3.3 Økende interesse for personvern blant foreldrene

Kommunene vi intervjuet, melder om stor interesse for elevenes personvern blant foreldre. Foreldrene er opptatt av hvilke nettressurser og applikasjoner elevene får tilgang til. De går også til lærerne med sine spørsmål og bekymringer om personvern. Dette viser at god opplæring av lærere på dette området er viktig.

> «Mange foreldre har reagert på at elevene pålegges bruk av verktøy uten riktig behandlingsgrunnlag.»
>
> **Christian Sørbye Larsen, Skolesec / KS**

> «Det er viktig med tillit til skolen slik at foresatte slipper å vurdere personvernet i hvert enkelt undervisningsopplegg. Det krever at skolen gjør seg fortjent til tilliten.»
>
> **Datatilsynet i Personvernpodden 4. mars 2021**

Under koronatiden har det vært en utfordring at det ikke er de samme sperrene i hjemmenettverkene som de har på skolen.

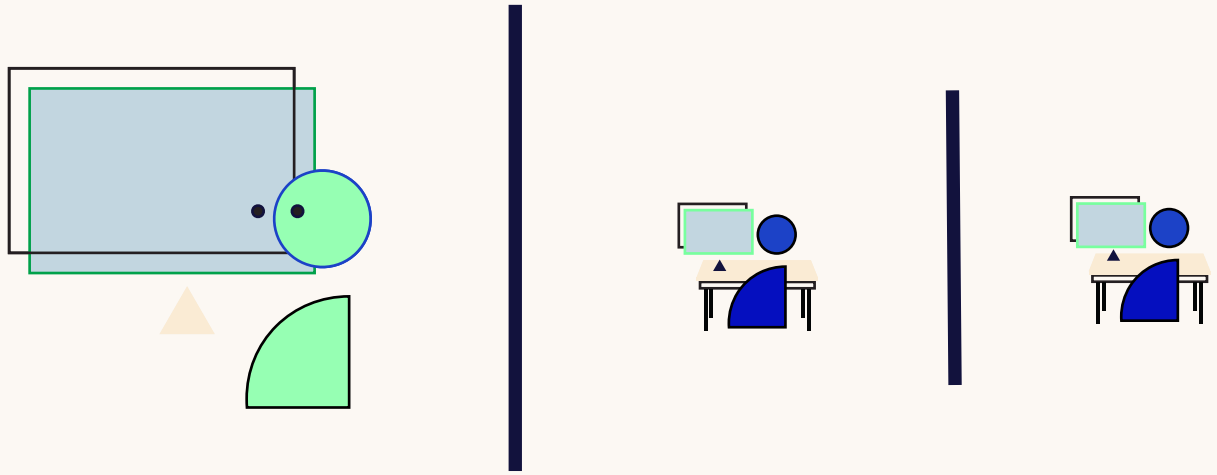
# 4 Situasjoner i skolen der personvern blir satt på prøve

I undersøkelsen vår har vi tatt utgangspunkt i ulike situasjoner i skolen der personvernet kan bli satt på prøve. Disse situasjonene er:

1. Bruk av digitale læringsressurser i undervisningen.
2. Digital innlevering av elevarbeid med digital tilbakemelding og vurdering fra læreren.
3. Håndtering av særlige kategorier av personopplysninger så som barnevernssaker, behov for spesialundervisning, varslingssaker og mobbesaker.
4. Dialog mellom hjem og skole.
5. Den generelle bevisstheten rundt håndtering av elevinformasjon.
6. Når elevinformasjon har kommet på avveie.
7. Når foreldre ber om innsyn eller sletting av personopplysninger.

Under vil vi ta for oss hver av disse situasjonene og presentere hva vår datainnsamling forteller om personvern i hver av dem.

## 4.1 Bruk av digitale læringsressurser i undervisningen



Digitale læringsressurser kan være alt fra PDF-dokumenter og statiske nettsider uten pålogging til avanserte interaktive verktøy der elevene løser oppgaver, bygger ting eller gjør simuleringer. Mange læringsressurser er laget spesielt for skolen. Men det er også mange andre ressurser på nettet som lærere ser det som nyttig å bruke i undervisningen, selv om de ikke er laget primært for skolen.

Personopplysninger som behandles i læringsressurser inkluderer:

- Informasjon som registreres i forbindelse med opprettelse av brukerkonto. Det kan være navn, bilde, kontaktinformasjon, kjønn, alder og lignende.
- Informasjon om elevenes faglige progresjon og resultater i verktøyet. Dette kan være informasjon som brukes for å tilpasse verktøyet til eleven.
- Dersom verktøyet inneholder reklame (noe det ikke bør dersom den skal brukes i skolen), så kan det registreres hvilke reklamer eleven har klikket på.
- Annen informasjon om elevens adferd i verktøyet.
- Elevenes geolokasjon.

## 4.1.1 Personvernkrav, risikoanalyser og databehandleravtaler

> «Kommunene rapporterer at de møter en jungel av digitale læringsressurser både fra nasjonale og internasjonale tilbydere. Uten god kompetanse om det som kjøpes inn, risikerer innkjøpene å bli mer tilfeldige.»
>
> **Pressemelding fra Kunnskapsdepartementet 2. desember 2020**

> «Det er helt andre krav knyttet til å kjøpe digitale læremidler sammenlignet med det å kjøpe bøker»
>
> **Christian Sørbye Larsen, Skolesec / KS**

Som i andre systemer som lagrer personopplysninger, må skoleeier som behandlingsansvarlig ha «en grunnleggende oppfatning om at behandlingen av personopplysninger er tilfredsstillende gitt deres behov for sikring»[7]. Dette får man blant annet ved å gjennomføre risiko- og sårbarhetsanalyser (ROS). Siden personopplysningene som regel lagres i leverandørens system, vil leverandøren ha rollen som databehandler. Dermed trengs også en databehandleravtale.

Arbeidet med ROS og databehandleravtaler har vært svært arbeidskrevende for skoleeierne. Blant tingene skoleeierne rapporterer at de sjekker, er:

- Hvor leverandøren holder til.
- Om det finnes hjemmel for utveksling utenfor EØS.
- Om utleveringsavtale med tredjepart er på plass.
- Om det er mulig for elevene å laste opp bilder eller legge inn sensitiv informasjon i kommentarfelter.

En av de vi intervjuet, anslo at ROS for en læringsressurs tar minst fem timer og at to personer bør involveres. Dette gir 10 timers arbeid. Med 13 – 16 fag, 10 klassetrinn og minst en læringsressurs per fag per klassetrinn så sier det seg selv at dette er svært arbeidskrevende. Små kommuner har ofte bare en rådgiver på skolekontoret i tillegg til oppvekstsjefen. De aller minste har kanskje ikke noen i det hele tatt.

---

7 Jarbekk og Sommerfeldt: *Personvern og GDPR i praksis,* side 127, CappelenDamm forlag

I kommunene vi snakket med, lot de lærere som foreslo nye verktøy, gjøre deler av analysen selv. Flere kommuner fortalte om at de likevel hadde et etterslep av læringsressurser som de trenger å vurdere.

> «Lærerne ønsker applikasjonene fort, gjerne i morgen»
>
> *Representant for skoleeier*

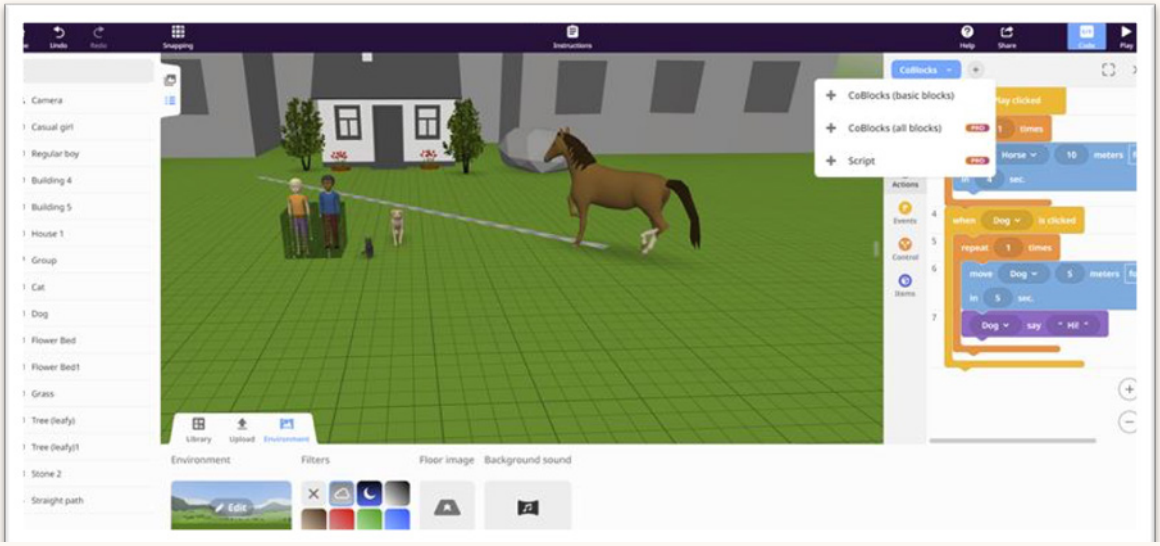
> «Hvis man skulle gjøre ROS-analyse av alle digitale læremidler, så ville man ikke få tid til annet.»
>
> *Lærer*

Også databehandleravtalene innebærer mye arbeid. I mange tilfeller er de komplekse og på engelsk. Det var tydelige signaler for våre intervjuobjekter om at de ikke har kompetanse og kapasitet til å håndtere alt dette.

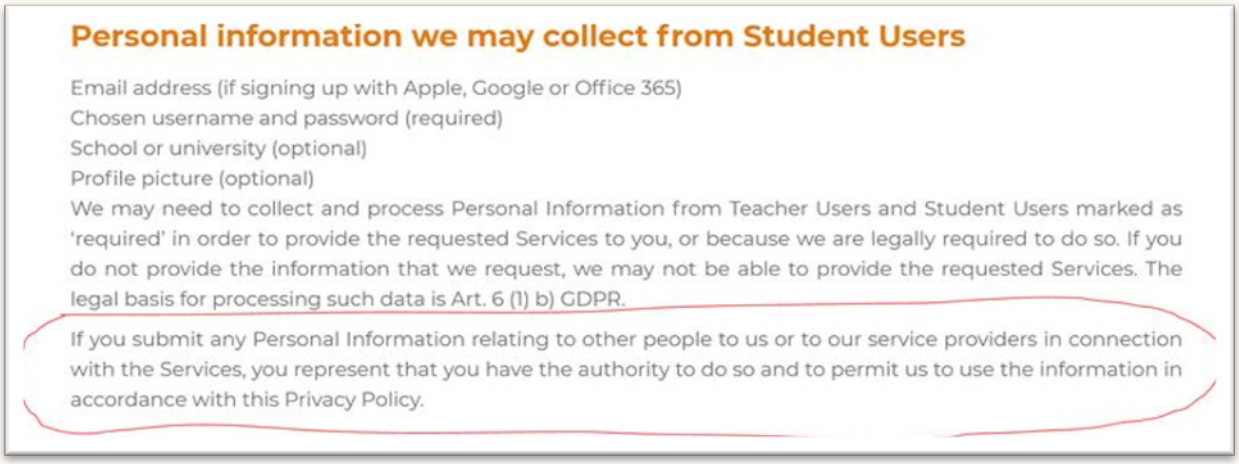
Vi har sett nærmere på noen av tjenestene som lærere tipset hverandre om på Facebook. Under har vi beskrevet utfordringer knyttet til vurdering av personvern i disse.

**Eksempel 1: Tøff tjeneste med tvilsom personvernerklæring**

Tjenesten CoSpaces (www.cospaces.io) er en gratistjenestene der elevene kan skape tredimensjonale miljøer, historier og spill som man kan bevege seg i (Virtual Reality).



Tjenesten har en personvernerklæring (se under) som sier at dersom elevene legger inn informasjon om andre personer, så er det i seg selv en bekreftelse på at de har tillatelse til å gjøre dette. Dessuten gir eleven da CoSpaces rett til å benytte denne informasjonen i tråd med deres policy. Dette er en formulering som det ikke er lov til å bruke i en personvernerklæring.



**Personal information we may collect from Student Users**

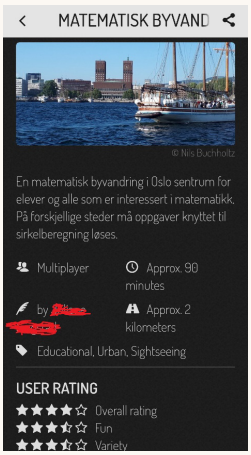
Email address (if signing up with Apple, Google or Office 365)
Chosen username and password (required)
School or university (optional)
Profile picture (optional)
We may need to collect and process Personal Information from Teacher Users and Student Users marked as 'required' in order to provide the requested Services to you, or because we are legally required to do so. If you do not provide the information that we request, we may not be able to provide the requested Services. The legal basis for processing such data is Art. 6 (1) b) GDPR.

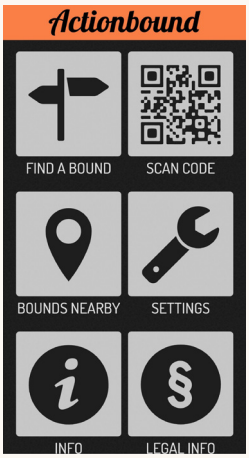
If you submit any Personal Information relating to other people to us or to our service providers in connection with the Services, you represent that you have the authority to do so and to permit us to use the information in accordance with this Privacy Policy.

**Eksempel 2 – Er det greit at bilder og tekst fra elevene lagres i USA?**

Floop (www.floopedu.com) er et annet verktøy som er anbefalt i Facebook-grupper for lærere. Det er et verktøy for å gi tilbakemelding til elever. Her kan elevene laste opp PDF-er, Google-dokumenter eller bilder av besvarelsene sine. Elev og lærer kan så ha en dialog om denne innleveringen.
Siden det lastes opp både bilder og fritekst, så innebærer bruk av tjenesten en personvernrisiko. Dataene lagres i USA og det er lite trolig at en liten norsk kommune vil kunne få en databehandleravtale med selskapet. Her er det definitivt behov for å vurdere personvernkonsekvenser (DPIA). Det er ikke lett for en norsk kommune å vurdere om bruk av et slik verktøy er greit.

**Eksempel 3 – Er det alltid feil med apper som bruker elevenes geolokasjon?**
ActionBound (www.actionbound.com) er en tjeneste der lærere kan lage rebusløp i lokalmiljøet med innlagte oppgaver på hver post. Dette gir mulighet for å bruke steder i lokalmiljøet i opplæringen samtidig som det gir en lekende tilnærming til læringen («gamification»).
Elevene løser oppgaven ved bruk av en mobilapp.




*En lærer har brukt ActionBound til å lage en matematisk byvandring i Oslo for skoleelever.*

Appen bruker lokasjonen til eleven for å avgjøre om de har kommet fram til riktig sted. Men er det greit å bruke apper som holder oversikt over hvor elevene er? Ålesund kommune fikk jo bot fra Datatilsynet for å be elevene bruke Strava som også sporer elevenes posisjon.

En av kommunene vi intervjuet, fikk anbefaling om å bruke ActionBound fra et universitet de samarbeider med. Kommunen kontaktet Datatilsynet og ble frarådet bruk av appen i skolen av personvernhensyn.

Vår utprøving viser imidlertid at ActionBound trolig ikke bryter med personvernet dersom det brukes på riktig måte. Selskapet er underlagt strenge lover i Tyskland og har tatt design-grep som sikrer personvernet. Appen registrerer hvilken elevgruppe som har funnet hvilke poster, men registrerer ikke bevegelsesmønster utover det. Det er ikke nødvendig for elevene å opprette brukerkonto og de kan gjerne bruke et kallenavn i stedet for sitt eget. Hvis man ikke har med oppgaver der elevene skal laste opp foto, så kan vi ikke se at denne appen innebærer større personvernrisiko enn for eksempel Kahoot.

Dette er et eksempel på en vurderinger det kan være vanskelig å gjøre for hver enkelt kommune. Resultatet kan lett bli at kommuner sier nei til å bruke gode og trygge verktøy for sikkerhets skyld. Dermed får elevene dårligere verktøy enn de ellers kunne fått.

**Innstramming i løpet av koronaåret – lærere opplever det som tungrodd**

Vårt klare inntrykk fra intervjuene er at skoleeierne det siste året har strammet inn bruken av digitale læringsressurser for å sikre at verktøyene har godt nok personvern. Mens det tidligere var vanlig at skolene selv vurderte hvilke verktøy som kunne brukes, så er dette nå sentralisert til skoleeier. Mange kommuner har lister av godkjente læringsressurser og formelle prosedyrer for å foreslå nye ressurser. En kommune melder at nye verktøy må godkjennes av rektormøte som gjennomføres to ganger per år. Både lærere og representanter for skoleeiere som vi intervjuet, opplever dette som tunge prosesser.

> «Hadde vi hatt mer tid, kompetanse og rutiner, så kunne lærerne fått tilgang til flere verktøy enn de får i dag. Dette er noe skoler og lærere klager på.»
>
> **Representant for skoleeier**

Det er grunn til å tro at en del lærere tar i bruk gratistjenester i undervisningen uten å gjøre en ROS-analyse. Det kan være på grunn av manglende opplæring eller fordi de opplever godkjenningsprosessen som for tungrodd.

> «I engasjement så får lærere lyst til å ta mange nye verktøy i bruk. I en heftig hverdag så er det lett å ta snarveier.»
>
> **Representant for skoleeier**

Samtidig er vårt inntrykk fra intervjuene at det etter hvert er skapt større forståelse blant lærere for at gratistjenester kan innebære en risiko.

**Innlogging med Feide sikrer en viss seriøsitet, men garanterer ikke personvern**

De mest brukte verktøyene har innlogging ved hjelp av Feide. Feide er den nasjonale løsningen for sikker innlogging og datadeling i utdanning og forskning. Løsningen utvikles og driftes av det statlige aksjeselskapet Uninett i samarbeid med Utdanningsdirektoratet. For å få Feide-innlogging kreves det at tjenesten tilføyer merverdi innen forskning- og utdanningssektoren. I tillegg kreves det at skoleeier skriver en databehandleravtale med leverandøren. Men Uninett blander seg ikke inn i hva denne databehandleravtalen inneholder.

Feide har noen personvernmessige fordeler. Den sikrer gjennom tofaktor-autentisering at de som logger seg inn, er de de utgir seg for å være. Feide gjør også at det ikke trengs e-postadresse som brukernavn ved innlogging. Feide-innlogging sikrer en viss seriøsitet av leverandøren, men er ingen garanti for at personopplysninger ikke kommer på avveie og at de håndteres på korrekt måte.

## 4.1.2 Kategorier av digitale læringsressurser

Vi har i vår datainnsamling sett at digitale læringsressurser faller i tre grupper når det gjelder håndtering av personvern:

1. Læringsressurser som dekker store deler av et fag. Dette er typisk læreverk utgitt av forlag som supplement til eller erstatning for lærebøker i faget.
2. Lisensbelagte applikasjoner for å lage bestemte typer oppgaver eller som dekker enkelttemaer innenfor et fag.
3. Gratis applikasjoner og tjenester på nett som passer til bruk for enkelttemaer innenfor fag eller enkelte typer oppgaver.

**Kategori 1: Læringsressurser som dekker store deler av et fag**

Dette er verktøy der det er relativt lite arbeid knyttet til vurdering av personvern sett opp mot bruken av verktøyene. Slike læringsressurser leveres av norske aktører som lever av tillit fra kundene sine. Kommunene vi har intervjuet, melder ikke om problemer knyttet til denne typen læringsressurser.

**Kategori 2: Lisensbelagte applikasjoner for enkelttemaer eller spesifikke formål**

Så lenge applikasjonene har en lisenskostnad, så tvinges beslutningene om bruk oppover i skolesystemet. Dermed øker også sannsynligheten for at det gjøres en personvernvurdering av verktøyet. Det er i denne kategorien det har vært mest innstramninger på bruken det siste året hos de vi har intervjuet.

I denne kategorien finnes mange utenlandske verktøy. For utenlandske verktøy rapporterer skoleeierne at det er vanskelig å få til en databehandleravtale. Dermed må man ta stilling til generelle «terms of service». Som eksemplene over viser, så kan dette være svært utfordrende vurderinger. For løsninger som har innlogging med Feide, så oppleves vurderingen som noe enklere for skoleeierne.

### Kategori 3: Gratis applikasjoner og tjenester på nett

> «Det var stort ønske om å ta i bruk gratistjenester. Vi følte at vi var festbrems.»
>
> **Representant for skoleeier**

> «I starten var det et voldsomt sinne over å ikke kunne ta i bruk gratis apper. Lærerne var vant til å kunne prøve ut på egen skole.»
>
> **Representant for skoleeier**

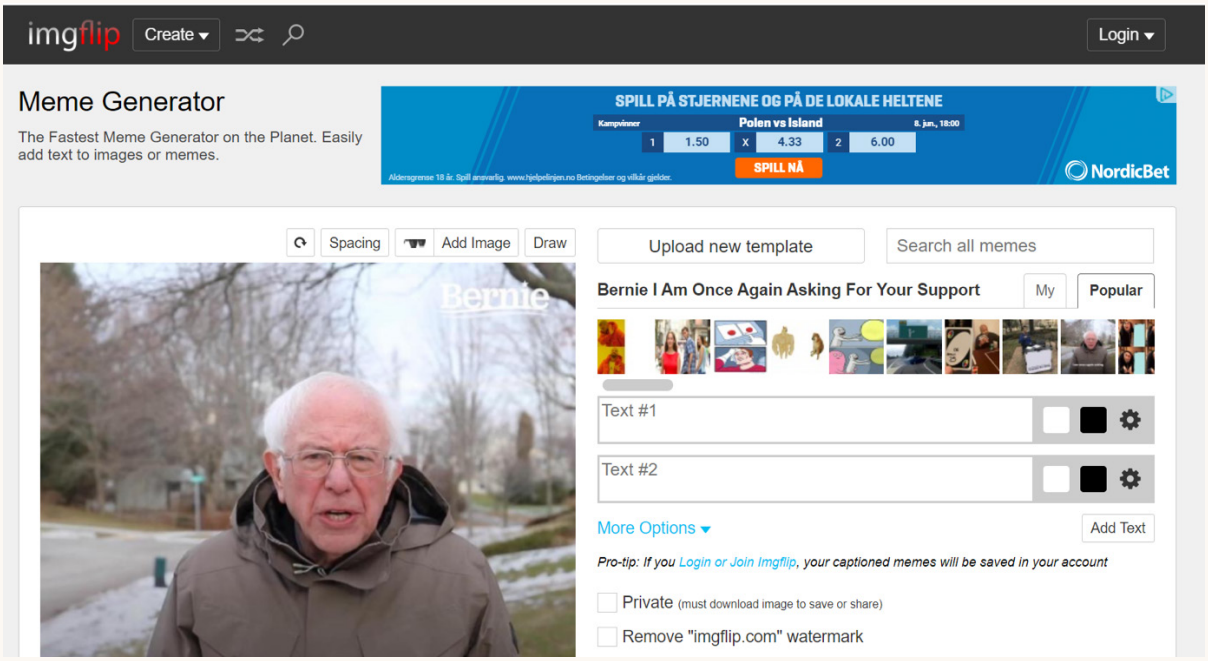
Skoleeierne vi snakket med, rapporterer om stort trykk fra lærere som ønsket å ta i bruk gratis digitale læringsressurser. Mange leverandører åpnet for gratis bruk av tjenestene da skolene stengte ned i mars 2020. Dette gjorde trykket enda større.

Gratistjenestene på nett er etter vår vurdering den kategorien verktøy der personvernrisikoen er høyest. Dette er tjenester som det er fristende å ta i bruk fordi de er gratis og enkelt å komme i gang. Samtidig er det klart at produsentene av disse tjenestene må leve av noe. Det kan være at de må selge reklame eller de kan selge informasjon om brukerne sine videre (for eksempel til andre aktører som selger reklame). En del gratis nettsider og tjenester på nett er offentlig finansiert (for eksempel de som er laget av universiteter), og dermed er risikoen mindre.

> Vi har ikke fått noen oppskrift på hvordan vi kan sjekke ut sikkerhet i gratis-apper.
>
> **Lærer**

#### Eksempel: Anbefalt læringsressurs viser reklame for pengespill

Mange av verktøyene som lærerne tipser hverandre om på Facebook, inneholder reklame. En lærer tipset om at hun som del av språkundervisningen hadde gitt elevene i oppgave å lage memes ved hjelp av tjenesten *imgflip*. Da vi gikk inn på tjenesten fikk vi opp reklame for pengespillet NordicBet:




Visning av reklame er i seg selv ikke et brudd på personvernet, men dersom elevene klikker på disse reklamene, er det sannsynlig at adferden deres vil bli lagret og eventuelt solgt videre. Det er også en risiko for at nettstedet selv tjener penger på salg av brukernes personopplysninger og adferd. Slik salg av opplysninger om personers adferd på nett, er noe Forbrukerrådet har satt søkelys på gjennom deltakelse i kampanjen Out of control[8].

Andre verktøy med reklame det er tipset om i gruppa, er språklæringstjenestene *K5 Learning* og *Duolingo*, samt geografispillet *GeoGeussr*.

> «Vi har en situasjon der barnas personopplysninger brukes som betaling for å få bruke gratisløsninger»
>
> *Christian Sørbye Larsen, Skolesec / KS*

## 4.1.3 Lærerne kan følge alt elevene gjør – Er det en ønsket utvikling?

I mange av verktøyene er det mulig for lærerne å følge elevenes progresjon tett og se hva elevene holder på med i verktøyet. Ett av matematikkverktøyene vi undersøkte, reklamerte med at læreren kan følge alle utregninger til hver enkelt elev. Det er lett å se at dette kan være en fordel for læreren. Dermed kan læreren følge med på elevens progresjon, gi relevant veiledning og tilbakemelding raskt.

8 https://www.forbrukerradet.no/out-of-control/


Samtidig virker denne typen overvåkning av elevene inn på deres arbeidsmiljø. Vi savner en diskusjon om hvorvidt dette er en hensiktsmessig utvikling.

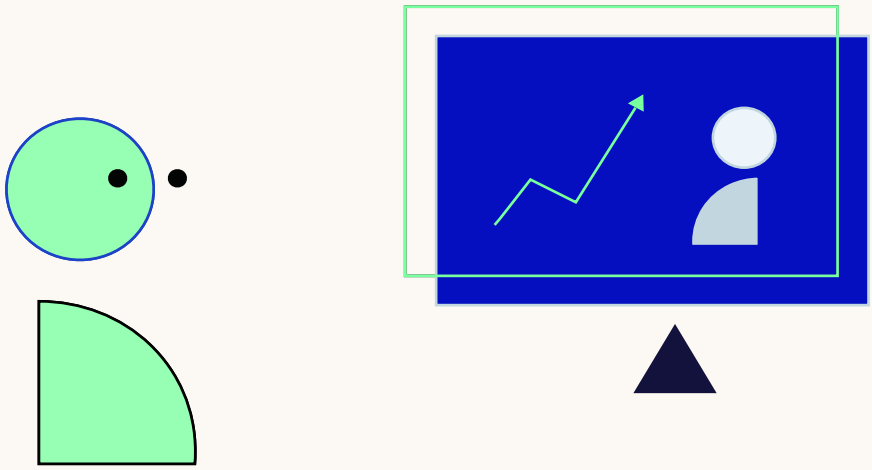
## 4.14 Oppsummering av utfordringer knyttet til digitale læringsressurser

- ROS-analyse, databehandleravtaler og sjekk av vilkår er svært ressurskrevende. Det oppleves som ressurssløsing at hver enkelt kommune må gjøre dette for hvert enkelt verktøy i hvert enkelt fag på de ulike klassetrinnene.
- Lærerne opplever kommunenes vurdering av de digitale læringsressursene som tungrodd og langsom. Det fører til at lærerne mister metodefriheten og at elevene ikke får så gode verktøy som de ellers kunne fått.
- Det er størst risiko for brudd på personvernet ved bruk av gratistjenester. Det er grunn til å tro at en del lærere tar i bruk gratisverktøy uten å gjøre vurdering av personvernet i verktøyet. Det skyldes ikke uvilje, men manglende opplæring og en svært travel hverdag.
- Reklame i pedagogiske verktøy innebærer en risiko for at elevene trekkes til nettsteder de ikke burde ferdes og der deres personopplysninger blir brukt til kommersielle formål.
- I en del digitale verktøy er det slik at lærerne kan følge tett med på alt elevene gjør. Det trengs en debatt om dette er en ønskelig utvikling.

«Usikkerhet rundt personvern på grunn av manglende kompetanse eller kapasitet kan være til hinder for god og trygg digitalisering. Usikre skoleeiere kan velge å ikke anskaffe og ta i bruk gode tjenester. Samtidig kan manglende kompetanse øke risiko for at løsninger med svakt personvern blir tatt i bruk. Dette kan igjen føre til forskjeller i elevenes tilgang til trygge, gode og likeverdige tjenester ut fra hvor i landet de bor.»

*Regjeringens handlingsplan for digitalisering av grunnopplæringen (2020-2021)*

## 4.2 Innlevering, vurdering og tilbakemelding for elevarbeid



For digital innlevering av elevarbeid og tilbakemeldinger fra lærerne brukes først og fremst de store læringsplattformene. Dette er tjenester som Google Worksuite for Education, Microsoft Office 365, itslearning og Showbie. De siste åra har de store internasjonale aktørene gjort et sterkt inntog på det norske markedet. Dette har ført til flere utfordringer knyttet til personvern. Datatilsynet ga irettesettelse til tre kommuner for måten de brukte Googles løsning. I den forbindelse uttalte direktør Bjørn Erik Thon:

– De som tar i bruk Google eller andre tjenester må vite hva dette innebærer for elevenes personvern. De må ha oversikt over hvilke data som samles inn, og hva de brukes til. Først da har du full oversikt over hva som står på spill for elevene. Det har kommunen ikke gjort i dette tilfellet.

Det har også vært saker knyttet til hvor i verden Showbie lagrer dataene sine og hva slags data som behandles i Showbie.

> «En kommune kan ikke alene stille krav til store amerikanske leverandører.»
>
> **Datatilsynet i Personvernpodden 4. mars 2021**

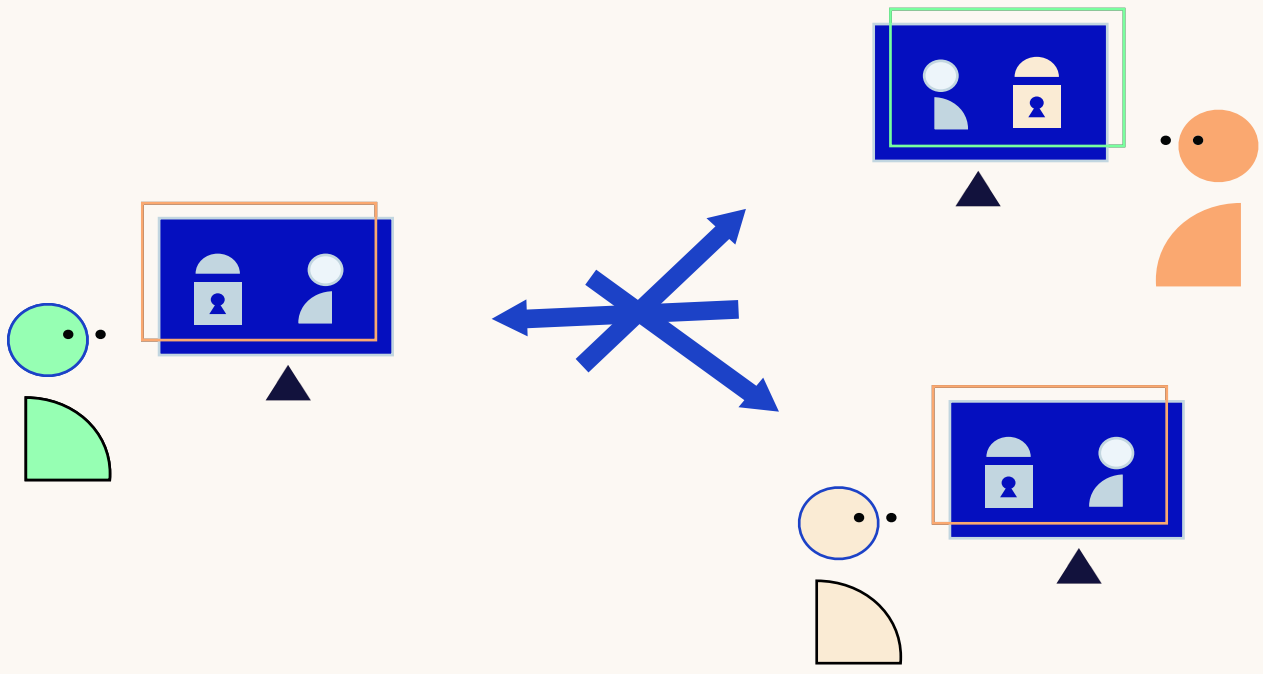
**E-postadresser til alle elever innebærer en risiko for svindel**

På skoler der elevene bruker Google eller Microsoft sine plattformer, så får alle elevene en e-postadresse fra skolen som de bruker til å logge seg inn med. Disse e-postadressene kan elevene bruke til å opprette kontoer på andre apper eller tjenester.

> «Vi har tilfeller der elevene har brukt e-postadresse fra skolen til å opprette konto på TikTok.»
>
> **Representant for skoleeier**

Slik bruk av e-postadressen kan føre til at elevene får e-poster med svindelforsøk eller phishing. Barn er ekstra sårbare for slike angrep det er vanskeligere for dem å vurdere hva som er seriøst og hva som er lureri.

## 4.3
## Håndtering av særlige kategorier av personopplysninger



Skoler håndterer en del personopplysninger som er mer sensitive enn elevenes karakterer og faglige progresjon. Eksempler på dette er helseopplysninger, individuelle opplæringsplaner (tidligere kjent som «spesialundervisning») og informasjon om mobbesaker, bekymringsmeldinger og barnevernssaker.

Vårt inntrykk fra intervjuene er at både skoleledere og lærere er bevisste på at dette er informasjon man må være svært forsiktig med. Dersom for eksempel diagnoser kommer på avveie, kan dette henge ved eleven hele livet. Kommunene har egne systemer for håndtering av denne informasjonen i form av sikre servere eller sak/arkiv-systemer med tofaktor-innlogging. Det er likevel flere problemer knyttet til håndtering av slik informasjon.

**De sikre løsningene er tungvinte eller lite tilgjengelig**

Flere av kommunene rapporterer om tungvinte og arbeidskrevende løsninger for håndtering av sensitiv informasjon. På en skole var det bare rektor som hadde tilgang sak/arkiv-løsningen der slik informasjon skal ligge. Det gjør at rektor for må skrive ut informasjon om mobbesaker og lignende på papir og distribuere disse fysisk til ansatte som jobber med eleven. Det har vært en utfordring under korona.

**Tungvint dialog med andre etater i kommunen**

Flere lærere og skoleeiere forteller at det er svært tungvint å sende personinformasjon mellom enheter i kommunen. Dette kan for eksempel være kommunikasjon med helsetjenester eller PP-tjeneste.

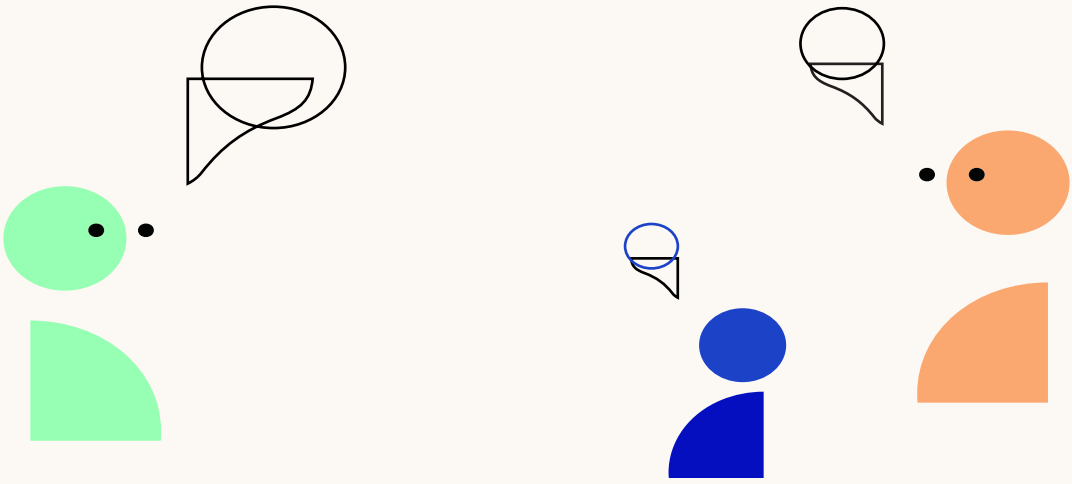
**Tungvinte løsninger skaper skyggeløsninger**

Det er et vanlig problem at tungvinte løsninger gjør det fristende å ta snarveier. En av skolene vi snakket med, la informasjon om mobbesaker i en notatblokk i OneNote beskyttet med et passord som ble spredt muntlig blant lærerne. Det er lett å se for seg at denne informasjonen kommer på avveie. Det er heller ikke heldig i et lokalsamfunn at alle lærerne har tilgang til slik informasjon for hele skolen.

På en skole skriver lærerne individuelle opplæringsplaner lokalt på egen PC, men uten forsiden med navn på eleven. Når den er ferdig, lages forsiden slik at planen kan lastes opp på sikker server. Deretter slettes forsiden med navnet. Det sier seg selv at ting kan glippe i slike manuelle løsninger.

> «Vi må være ærlig på at vi bruker e-post også i mobbesaker. Men vi prøver å ikke navngi i e-poster og sier at ”det har vært en episode” og så ringes vi heller.»
>
> **Lærer**

# 4.4 Dialog mellom skole og hjem



I koronatiden har dialogen mellom skole og foresatte endret seg. Mange utviklingssamtaler har blitt gjennomført på video. En rekke kommuner har også innført egne sikre løsninger for dialog mellom skole og hjem

**Er Teams sikkert nok videomøter med sensitiv personinformasjon?**

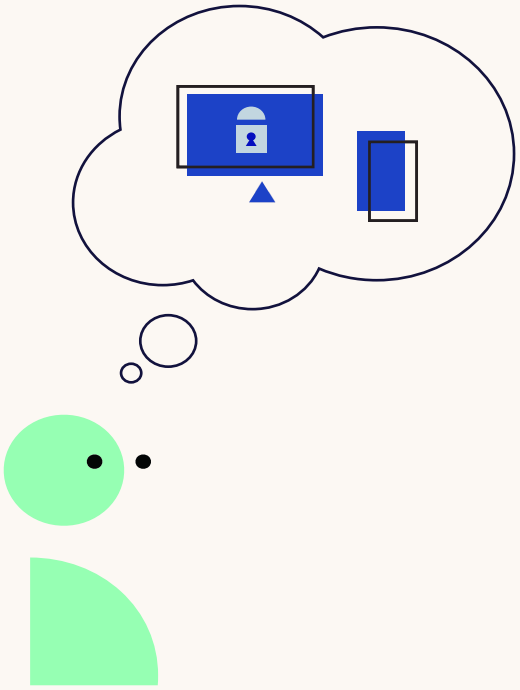
Noen av kommunene vi snakket med, hadde tatt i bruk ekstra sikre videoløsninger for utviklingssamtaler med sensitiv informasjon. For slik samtaler vurderte de ikke Microsoft Teams som sikkert nok. Det er positivt at kommunen gjør slike vurderinger, men en av lærerne kommenterte at det førte til at han måtte lære seg og bli trygg på nok en IT-løsning i sin skolehverdag.

«Kommunikasjon mellom hjem og skole må være sikker»

**Bjørn Erik Thon, direktør i Datatilsynet**
**I podkasten til Christian Lomsdalen 9. februar 2021**

«De fleste foreldre anser e-post som sikkert. Andre verktøy er det vanskelig å få foreldrene til å bruke. De er veldig på e-post.»
**Lærer**

# 4.5 Bevissthet i hverdagen



Det hjelper ikke med sikre systemer dersom brukeren sender eller lagrer personopplysninger på feil måte. *Hvordan systemene brukes* er minst like viktig som hvordan systemene er utformet. Riktig håndtering av personinformasjon krever ikke bare teknisk opplæring i en rekke systemer, men det krever også at lærere og skoleledere forstår *hvorfor* personvern er viktig.

Gjennom intervjuene har vi fått inntrykk av at lærerne har høy grad av bevissthet om at personinformasjon må håndteres med forsiktighet. Taushetsplikten er noe lærerne har hatt i over hundre år. Det ser også ut til å være godt innarbeidet at man ikke skal bruke navn på elevene i e-poster og annen skriftlig dialog.

Men i en tid med akselererende digital utvikling er det mange nye systemer, regler og rutiner lærerne må sette seg inn i. Det å vurdere om et informasjonselement kan sendes i en gitt kommunikasjonskanal eller om en digital læringsressurs har tilstrekkelig innebygd personvern krever en ny type kompetanse og bevissthet. Alle kommunene vi snakket med forteller om stort strekk i laget på dette området.

**Eksempler på ting som kan gå galt i hverdagen**

I intervjuene har vi hørt om ulike situasjoner der det glipper. Det kan for eksempel være at en elev er invitert inn i et Teams-møte for å diskutere en sak med noen lærere. Dermed får eleven tilgang til chatten mellom lærerne selv etter at han eller hun har forlatt møtet. Et annet problem er varsler som kommer opp på lærerens datamaskin mens læreren viser noe på storskjerm i klasserommet. Slike varsler kan lett inneholde personinformasjon.

«Med den lille opplæringen jeg har hatt, så føler jeg ikke at jeg har kontroll på Teams ennå.»

*Lærer*

«Det er veldig mye en lærer skal kunne. Hvis det forventes at lærere skal kunne personvernregler og fallgruver, så blir det veldig mye.»

*Lærer*

«Dersom 40 slitne lærere får et totimerskurs i personvern en onsdag kveld, så glemmer vi det fort.»

*Lærer*

«Det er to ting alle lærere må kunne. Det er skrive på tavla og det er innholdet i GDPR artikkel 5.» (Prinsippene som ligger til grunn for GDPR. Red. anm.)

*Christian Sørbye Larsen, KS/Skolesec*

«Det største problemet er lite kunnskap og forståelse for hvorfor personvern er viktig. Da oppleves alt som tungvint. Bevisstheten er på vei til å bli bedre, men dette er noe vi må jobbe med.»

*Representant for skoleeier*

«Vi har årshjul der rektorene må kvittere ut at de har informert lærerne om rutiner. Men det er en utfordring å nå ut til alle ansatte med bevissthet. Bevisstheten blant de ansatte er den største sikkerhetsventilen vår»

*Representant for skoleeier*

**Tungvinte løsninger presser fram snarveier**

I en presset hverdag er det lett å ta snarveier dersom systemene blir for tungvinte. Dette er noe vi fikk bekreftet i intervjuene.

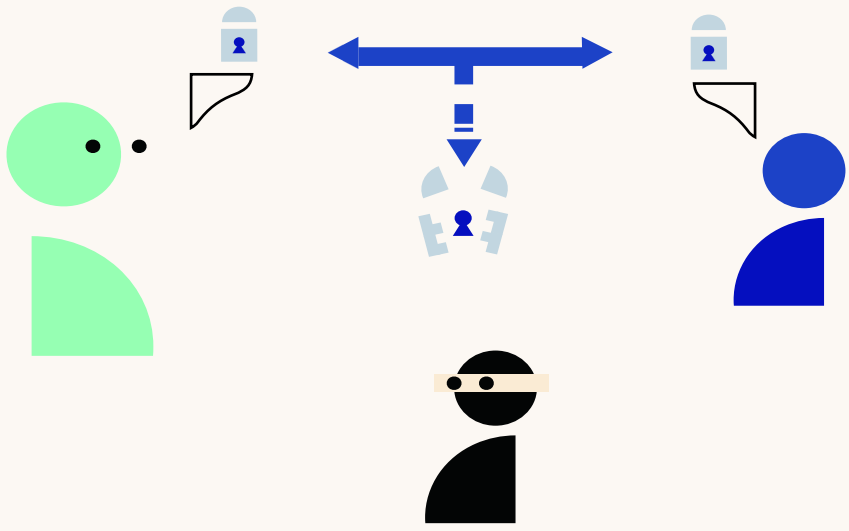
> «De fleste lærerne holder seg til reglene. Men det er nok noen som tar noen snarveier for at ikke arbeidshverdagen skal bli for tungvint»
> *Lærer*

> «Noen av personvernreglene er ikke mulig å håndtere i praksis»
>
> *Rektor*

> «Noen lærere synes personvern er tungvint.»
>
> *Representant for skoleeier*

> «Alt som kommer i veien for undervisningen, oppleves som prakk og unødvendig. Det er ikke uvilje, men det er mange ting som kommer lenger opp på lista for lærerne enn personvern.»
> *Representant for skoleeier*

## 4.6 Når elevinformasjon har kommet på avveie

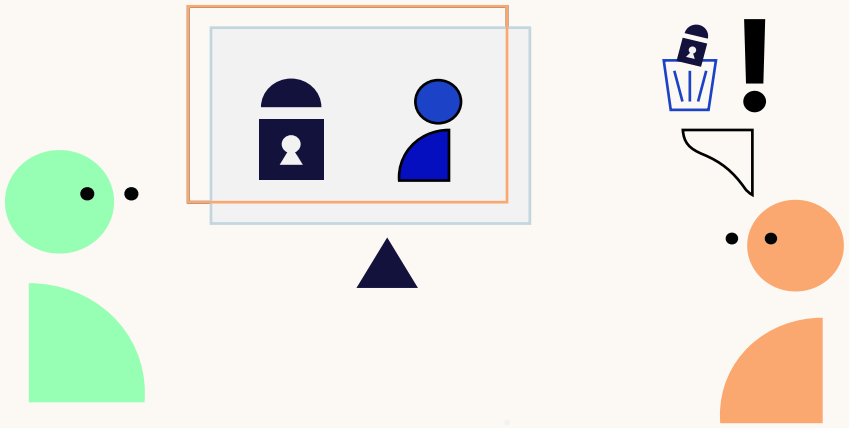


Den nye personopplysningsloven setter konkrete krav til hva som skal gjøres dersom noe går galt og personinformasjon kommer på avveie. Blant annet skal det meldes fra til Datatilsynet uten ugrunnet opphold innen 72 timer etter at man har fått kjennskap til bruddet.

Flere av kommunene vi snakket med, har avvikssystemer der brudd på personvernet skal registreres. Men ingen av lærerne vi intervjuet, kjenner til rutiner for hva man skal gjøre ved brudd på personvernet. Også hos representantene for skoleeierne var inntrykket at slike rutiner er lite kjent og lite i bruk på skolen og på kommunens skolekontor.

> «Vi har et avvikssystem, men jeg kan aldri tro at det blir brukt i praksis.»
>
> *Representant for skoleeier*

## 4.7 Når foreldre ber om innsyn eller sletting av personopplyninger



Personopplysningsloven fra 2018 gir nye rettigheter til innbyggerne når det gjelder innsyn og sletting av data om seg selv. I skolen, som i andre offentlige virksomheter, vil det være informasjon som ikke kan slettes av hensyn til arkiv, dokumentasjon og sporbarhet.

Flere kommuner vi snakket med, var redde for at antallet innsynsbegjæringer ville stige etter at den nye personopplysningsloven kom. Det har imidlertid ikke skjedd. Enkelte av kommunene har fått noen begjæringer om innsyn, for eksempel av personer som har bedt om dokumentasjon på hvilken skolegang og opplæring de har fått. Flere av kommunene har en personvernapplikasjon der de holder oversikt over hvilke personopplysninger som ligger i hvilke systemer. Det gjør det lettere å håndtere eventuelle innsynsbegjæringer.

> «Vi var redd for at begjæring om sletting og innsyn ville ta av, men vi har ikke mottatt noen slike.»
>
> *Representant for skoleeier i stor kommune*

# 5. Vurderinger og oppsummering

Vår gjennomgang har vist at skolesektoren ble stilt overfor store utfordringer da de først fikk ny personopplysningslov med detaljerte krav og deretter måtte legge om hele driften i forbindelse med korona. Her vil vi oppsummere våre hovedfunn.

## 5.1 Behov for opplæring og bygging av forståelse

Lærere og skoler har gjort en formidabel jobb i å legge om til heldigital skole. De har fått et stort digitalt kompetanseløft som vil ha stor nytte også etter korona.

Personvernet er godt ivaretatt internt i de store og mest brukte systemene i skolen. Risikoen ligger imidlertid i hva slags informasjon de ansatte velger å legge i hvilke systemer og kanaler.

For personvernet i skolen er det ikke nok at systemene har innebygd personvern. I tillegg må hver enkelt ansatt være bevisst på regler og risiko og ha kompetanse innenfor digitalt personvern. Intervjuene viser at det fortsatt er en stor jobb å gjøre på dette området.

> «Når en lærer har med seg en småskoleklasse på tur i byen, så har alle elevene gule vester, holder i et tau og det er nok voksne med på turen. Disse organisatoriske tiltakene ligger ryggmargen på lærerne. Den samme ryggmargsrefleksen vil jeg ha når de sender elevene ut på nettet også.»
>
> *Christian Sørbye Larsen, KS/Skolesec*

## 5.2 Ineffektiv vurdering av digitale læringsressurser gir elevene dårligere verktøy og innskrenker lærernes metodefrihet

I dag er det slik at hver av de 356 kommunene og 11 fylkeskommunene i Norge må gjøre egne risiko- og sårbarhetsvurderinger og sørge for gode nok databehandleravtaler med hver leverandør av læringsressurser for alle fag og alle klassetrinn. Det er mange flere momenter som må vurderes ved innkjøp av digitale læringsressurser sammenlignet med kjøp av skolebøker. Dette er noe skoleeierne ikke har tilstrekkelig kapasitet eller kompetanse til å gjøre. Resultatet er at kommunene må begrense hvilke verktøy lærerne får lov til å bruke og at lærerne får innskrenket sin metodefrihet.

I tillegg innebærer dette dobbeltarbeidet en ressurssløsing.

Flere av de vi har intervjuet, peker på at elever og lærere kunne fått tilgang til bedre verktøy dersom dette hadde vært løst på en annen måte.

Tungrodde rutiner for godkjenning av læringsressurser gjør det også mer fristende for lærerne å ta i bruk gratisressurser med uavklart personvern.

Ressurskrevende risikovurderinger og databehandleravtaler bidrar til forskjeller mellom kommunene. Små kommuner har ofte ikke samme kompetanse og kapasitet til vurdering av personvern i verktøy. Dette er et problem som også pekes på i regjeringens handlingsplan for digitalisering i grunnopplæringen (2020 – 2021)[9].

## 5.3 Stor risiko for personvernbrudd når gratis digitale verktøy brukes

Det finnes mange gratisverktøy på nett som kan egne seg for bruk i undervisningen. Leverandører som ikke har offentlig støtte, må tjene penger på en eller annen måte. Kommersiell bruk eller videresalg av brukernes personinformasjon og adferdsmønster er en måte de kan tjene penger. Gjennom Facebook-grupper har vi sett at mange lærere har tatt i bruk gratisapplikasjoner i løpet av koronatiden. Dette innebærer en risiko for elevenes personvern.

## 5.4 Håndtering av sensitive personopplysninger er tungvint og fører til sårbare skyggesystemer

Vi har sett at kommuner har systemer for håndtering av sensitiv personinformasjon informasjon og at det finnes en bevissthet blant ansatte rundt slik informasjon. Disse systemene er imidlertid tungvinte og ressurskrevende mange steder. Det fører til at andre løsninger brukes, noe som gir sårbarhet med tanke på personvern.

## 5.5 Ansatte på skoler vet ikke hva de skal gjøre dersom personinformasjon kommer på avveie

Personopplysningsloven setter krav til at brudd på personvernet skal meldes som avvik innen 72 timer. Våre intervjuer viser at det ikke er tydelig kommunisert ut til skolene hva som skal gjøres dersom personinformasjon har kommet på avveie.

## 5.6 Digitale verktøy gir innsyn i alt elevene foretar seg

Allerede i 2014 påpekte Datatilsynet faren for for mye overvåking av elevenes nettbruk i skolen. Mange digitale verktøy gir læreren full innsikt i det elevene foretar seg. Vi mener det trengs en debatt om hvordan dette påvirker elevenes arbeidsmiljø.

9 https://www.regjeringen.no/contentassets/44b8b3234a124bb28f0a5a22e2ac197a/handlingsplan-for-digitalisering-i-grunnopplaringen-2020-2021.pdf

# 6. Hva gjøres på feltet

Heldigvis finnes det flere som jobber for å hjelpe skoleeierne med håndtering av det digitale personvernet. Her vil vi nevne noen av disse.

## 6.1 Datatilsynet

Datatilsynet er først og fremst et tilsynsorgan. Men de driver også en god del informasjonsvirksomhet både på nettsidene sine, i Personvernpodden og i form av artikler og foredrag.

## 6.2 Skolesec fra KS

Skolesec er et prosjekt i regi av KS. Målet er å stille verktøy og ressurser til disposisjon slik at kommunene kan gjennomgå de læringsressursene og samhandlingsløsningene som brukes mest. Skolesec tilbyr blant annet:

- Sjekkliste for ROS-analyse
- Maler for databehandleravtaler
- Mal for gjennomføring av DPIA
- En treningsplattformfor styrking av kompetansen på personvern og informasjonssikkerhet i utdanningssektoren (https://trening.skolesec.no/)

## 6.3 Handlingsplan fra Kunnskapsdepartementet

I desember 2020 lanserte regjeringen en handlingsplan for digitalisering av grunnopplæringen. Der foreslår de blant annet at det etableres en felles nasjonal tjenestekatalog for digitale læringsressurser. Kunnskapsminister Guri Melby sa i forbindelse med lanseringen at de med denne handlingsplanen ønsker å bidra til å redusere forskjellene mellom kommunene gjennom tettere samarbeid mellom stat og kommunene[10].

## 6.4 GDPR-prosjekt fra Pålogga AS

Initiativtakerne til Facebook-gruppen Koronadugnad for digitale lærere har startet det ideelle aksjeselskapet Pålogga AS. De har lansert CheckIT som er en veileder for vurdering av personvern i læringsressurser og har gjort vurderinger av personvernet i en del digitale læringsverktøy.

10 https://www.regjeringen.no/no/aktuelt/vil-styrke-kommunenes-digitaliseringsarbeid-i-skolene/id2788319/

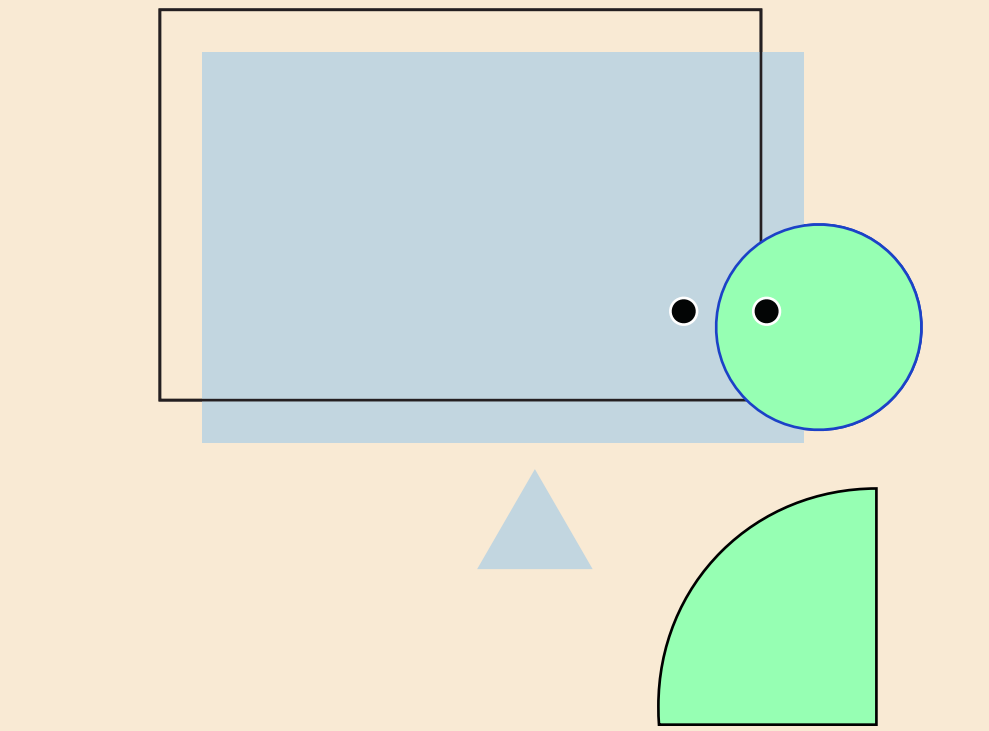
# 7. Hva mer bør gjøres

I denne rapporten har vi pekt på en rekke utfordringer knyttet til personvern i skolen. Skoleeiere og lærere står i en skvis mellom det å gi en best mulig undervisning og det å ivareta elevenes personvern på en tilstrekkelig måte.

Vi mener følgende tiltak må til for å sikre personvernet, gi bedre undervisning og utnytte ressursene bedre:

- Det er stort behov for å samordne og effektivisere arbeidet med risikoanalyser og databehandleravtaler for digitale verktøy. Dette kan gjøres ved å realisere en felles tjenestekatalog for digitale læringsressurser som regjeringen selv har foreslått i sin handlingsplan for digitalisering av grunnopplæringen. Slik vil mange flere elever og lærere i distriktene i Norge få tilgang til bedre verktøy. Et slikt grep vil også bidra til at verktøy som har for dårlig på personvern holdes utenfor norsk skole.
- Kompetansen og bevissthet om digitalt personvern hos lærere, skoleledere og skoleeiere må bygges systematisk. Norsk skole trenger tydelige kjøreregler som forklarer hvorfor personvern er viktig og hvordan det skal ivaretas.
- Systemer og rutiner for håndtering av sensitiv informasjon om elevene må på plass både internt i skolesystemet og i dialogen med andre instanser i kommunen. Krav til verktøy og forslag til rutiner som trygger de situasjonene vi gjennomgår i rapporten, bør utvikles sentralt slik at den enkelte lærer og skole slipper å ta utrygge valg.

Vi oppfordrer Utdanningsdirektoratet og Kunnskapsdepartementet til å komme på banen for å iverksette tiltak som nevnt over. KS er en organisasjon som kjenner skoleeiernes hverdag godt. En styrking av KS sin satsing på Skolesec vil derfor være et godt tiltak for å møte de utfordringene skolen står ovenfor når det gjelder personvern.



bouvet