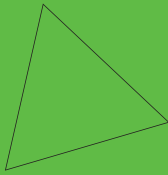
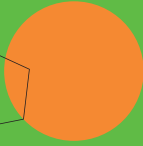
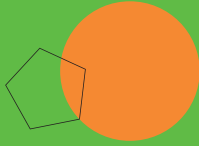
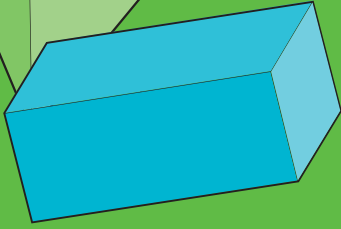
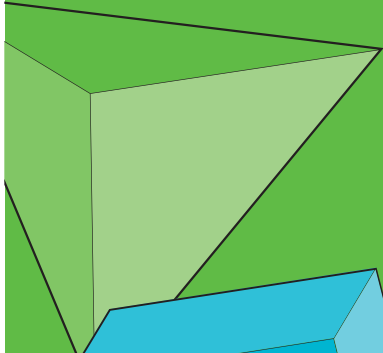


SENTER
FOR IKT I
UTDANNINGEN



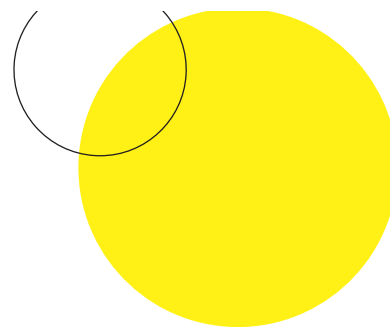
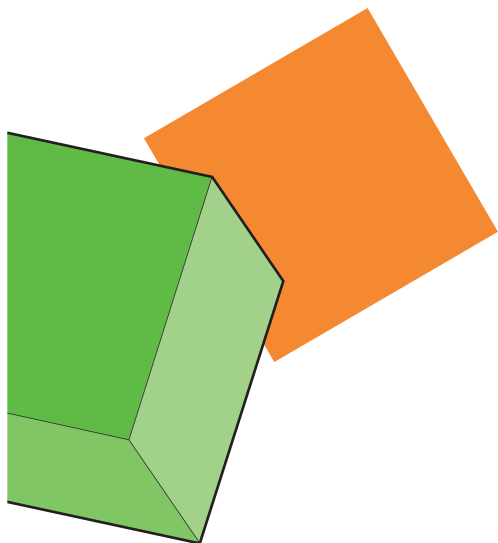
Informasjonssikkerhet i barnehagen

En veileder i håndtering av personopplysninger og viktig informasjon



Informasjonssikkerhet i barnehagen

En veileder i håndtering av personopplysninger og viktig informasjon



Forord

Senter for IKT i utdanningen er underlagt Kunnskapsdepartementet og arbeider for at informasjons- og kommunikasjonsteknologi (IKT) skal bidra til økt kvalitet og styrket læringsutbytte.

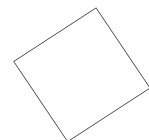
Et viktig strategisk og fremtidsrettet satsingsområde for Senter for IKT i utdanningen er økt satsing på bruk av IKT i barnehager. Det er et ønske at IKT skal være en sentral del av det pedagogiske tilbudet i barnehagen, hvor digitale verktøy bør være en kilde til lek, kommunikasjon og innhenting av kunnskap. En viktig oppgave for senteret er også å styrke den digitale kompetansen i utdanningsinstitusjoner uavhengig av brukernes sosiale bakgrunn og bosted.

Målet med veilederen

Målet med denne veilederen er å hjelpe ledere og ansatte i barnehager til å oppfylle sine lovpålagte plikter med hensyn til sikring av personopplysninger og å øke bevisstgjøringen rundt viktigheten av god informasjonssikkerhet. Gjennom økt forståelse og bedre kunnskap om dette vil man kunne unngå krenkelser av personvernet til ansatte, barn og foreldre. I tillegg vil det sikre at viktig informasjon i barnehagen blir håndtert på en sikker måte.

Metodisk utgangspunkt

Som utgangspunkt for veilederen, og for å dra lærdom av daglige situasjoner i barnehagen, har Senter for IKT i utdanningen utført kvalitative intervjuer i utvalgte barnehager hvor styrere og pedagogiske ledere er stilt spørsmål om informasjonssikkerhet. Senteret har også gjennomført en omfattende kvantitativ undersøkelse hvor resultatene er brukt til å kartlegge situasjonen når det gjelder informasjonssikkerhet i norske barnehager.





Innholdsfortegnelse

Forord 4

Introduksjon 6

Uønskede hendelser og sikkerhetstiltak 8

MUNTLIG DIALOG 8

E-POST 9

TEKSTMELDINGER 10

ARKIVSKAP 12

ELEKTRONISK LAGRING 13

MINNEPINNER 14

FJERNARBEIDSLØSNINGER 15

FOTO OG VIDEO 16

HJEMMESIDER 17

SOSIALE MEDIER 18

SKYTJENESTER 19

Ordliste 22





Introduksjon

I barnehager håndteres personopplysninger, det vil si alle typer informasjon og vurderinger om ansatte, barn og foreldre. Mye av dette skjer ved bruk av digitale verktøy og digitalt utstyr, eksempelvis administrative systemer, e-post, Internett og hjemmesider, bærbare og stasjonære datamaskiner og minnepinner. I tillegg er det svært vanlig at personopplysninger skrives ned på papir og oppbevares i arkivskap, eller kommuniseres daglig gjennom muntlige samtaler.

Alle barnehageeiere har en lovpålagt plikt til å sørge for at personopplysninger som behandles elektronisk, eller oppbevares i arkivskap, er tilfredsstillende sikret. Dette følger av personopplysningsloven § 13 og personopplysningsforskriften kapittel to, og omtales som informasjonssikkerhet. Formålet med reglene om informasjonssikkerhet er å unngå krenkelser av personvernet til ansatte, barn eller foreldre. Det vil si å ivareta behovet for personlig integritet og privatlivets fred. Målet med denne veilederen er å hjelpe barnehagepersonalet til å oppfylle sine lovpålagte plikter og sikre at personopplysningene blir håndtert på en forsvarlig måte.

Veilederen inneholder en rekke eksempler på hendelser som kan føre til brudd på informasjonssikkerheten, og inkluderer sikkerhetstiltak som kan iverksettes for å unngå dette. Den dekker likevel ikke alle uønskede hendelser eller aktuelle sikkerhetstiltak.

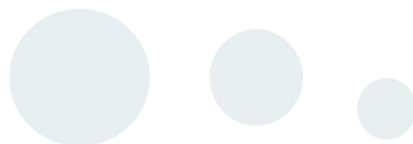
Hva menes med personopplysninger?

I personopplysningsloven defineres all informasjon og alle vurderinger som kan knyttes til en bestemt enkeltperson som personopplysninger. Opplysningene kan foreligge i form av tekst, bilder, film, video- eller lydopptak. All informasjon om navn, adresse, alder, telefonnummer, e-postadresser og fødselsnummer anses som personopplysninger. Det er også vanlig at saksdokumenter, utredninger, eller vurderinger som omhandler barnehagebarn inneholder denne typen opplysninger.

I personopplysningsloven skiller det mellom sensitive og alminnelige personopplysninger. Med sensitive personopplysninger menes informasjon om:

- Helse og helserelaterte forhold
- Etnisk eller rasemessig bakgrunn
- Politisk, religiøs eller livssynsoppfatning
- Seksuell legning
- Strafferettslige forhold
- Fagforeningsmedlemskap

Alle andre typer personopplysninger regnes som alminnelige.



Hvordan ivareta informasjonssikkerhet?

Personopplysningsloven § 13 krever at behandlingen av personopplysninger er tilfredsstillende sikret. Verdt å merke seg er at dette betyr at personopplysninger skal være tilfredsstillende sikret uavhengig av om de er sensitive eller alminnelige. Datatilsynet stiller likevel ekstra strenge krav til sikring av sensitive personopplysninger. Barnehageeier er selv pålagt å bestemme hva som helt konkret menes med at opplysningene er tilfredsstillende sikret. Kravene som barnehageeieren har utarbeidet skal være nedskrevet i barnehageeierens handlingsplan.

Det finnes tre typer uønskede hendelser som personopplysningene skal sikres mot. Disse er beskrevet som:

1. **Konfidensialitetshendelser:** Hindre at uvedkommende, (både i og utenfor barnehagen), får tak i opplysninger om ansatte, barn eller foreldre. Dersom andre enn de som har rett til å kjenne til opplysningene likevel får tilgang til dem, er det et brudd på opplysningenes konfidensialitet.
2. **Integritetshendelser:** Hindre at opplysninger om ansatte, barn eller foreldre endres eller slettes av personer som ikke er autorisert til å gjøre dette. Dersom andre enn de som har tillatelse endrer eller sletter personopplysninger, er det et brudd på opplysningenes integritet.
3. **Tilgjengelighetshendelser:** Sørg for at personopplysninger, til enhver tid, er tilgjengelige for de som har rett til og behov for å bruke dem. Dersom ansatte i barnehagen ikke får tak i opplysninger om kollegaer, barn eller deres foreldre er det et brudd på opplysningenes tilgjengelighet.



Uønskede hendelser og sikkerhetstiltak

MUNTLIG DIALOG

Alle barnehageansatte er underlagt forvaltningslovens krav til taushetsplikt, hvilket betyr at de er pliktige til å ivareta taushet rundt "noens personlige forhold". Styreren har plikt til å informere de øvrige ansatte om hvilke regler som gjelder. De ansatte bekrefter som oftest at de har kjennskap til reglene ved å signere en taushetserklæring. Hvor grensene går for hvilken informasjon som kan deles med alle de ansatte, og hva som må holdes tilbake, vil likevel ofte være en vurderingssak.

Barnehagen har liten kontroll med hva de ansatte sier til foreldrene, eller andre de måtte ha kontakt med, i eller utenfor barnehagen. Det er denne dialogen som er forbundet med størst risiko med hensyn til taushetsplikten. For å unngå uønskede hendelser er det viktig å ha et bevisst forhold til taushetsplikten og sikre at de ansatte er kjent med hvor grensene går.

Eksempler på uønskede hendelser som kan forekomme i forbindelse med muntlig dialog

- Ansatte får greie på informasjon de ikke burde hatt kjennskap til fordi de overhører samtaler mellom andre ansatte.
- Foreldre overhører samtaler ansatte imellom, eller mellom ansatte og andre foreldre, om forhold som de ikke burde vært kjent med.
- Det oppstår ryktespredning fordi muntlige beskjeder har blitt misforstått eller videreformidlet på feil måte.
- Ansatte snakker med bekjente utenom arbeidstid som da får greie på informasjon som skulle vært forbeholdt personer tilknyttet barnehagen.

Er du bevisst på hvor du er når du snakker om personopplysninger og sensitiv informasjon? Du vet aldri hvem som kan overhøre samtalen

Eksempler på sikkerhetstiltak for å unngå uønskede hendelser

- Ha klare retningslinjer for hvordan informasjon skal deles, og sørg for bevisstgjøring rundt hva taushetsplikten innebærer.
- Etabler rutiner for hvordan beskjeder og informasjon fra foreldre skal håndteres.
- Ha egnede rom for diskusjon av viktige og sensitive temaer.
- Vær bevisst på at viktige beskjeder blir formidlet på en måte som ikke kan misforstås.
- Vurder om viktige beskjeder og avgjørelser også skal foreligge skriftlig, for på den måten å unngå misforståelser.

Visste du at 32 % av norske virksomheter mener at informasjon har kommet på avveie på grunn av feilsendte e-post?



E-POST

E-post er en mye brukt kommunikasjonskanal i barnehager, spesielt i kommunikasjonen med foreldrene. E-post er effektivt til å informere foreldrene om månedsplaner, aktiviteter, retningslinjer, eller andre ting som gjelder alle barna i barnehagen. Det er enkelt å sende ut informasjon til mange på en gang via e-post. Den kommer raskt frem og kostnadene knyttet til utsending er ofte lave.

Hvis e-post benyttes til å sende viktig eller sensitiv informasjon, er det viktig å være klar over at dette er et usikkert kommunikasjonsmedium. Er ikke de riktige forholdsreglene tatt, kan det fort oppstå uønskede hendelser.

Eksempler på uønskede hendelser som kan forekomme ved bruk av e-post

- Ansatte i barnehagen, eller foreldre, sender sensitive opplysninger til feil e-postadresse slik at informasjonen blir tilgjengelig for uvedkommende.
- Foreldre, eller personalet i barnehagen, får ikke den informasjonen de skal ha fordi viktige beskjeder er sendt til feil e-postadresse.
- Uvedkommende får tilgang til sensitiv informasjon fordi ansatte har sendt dokumenter til sin private e-postadresse.
- E-poster med helseopplysninger, eller andre sensitive opplysninger, sendes til eksterne instanser (PPT, skole osv.) uten bruk av sikring (kryptering) og kan dermed potensielt leses av uvedkommende.

- Viktige e-poster kommer ikke frem til barnehagen fordi Internett ikke er tilgjengelig.
- Ansatte som ikke skulle hatt tilgang til barnehagens e-postkonto får tilgang til denne fordi det benyttes en felles datamaskin som automatisk logger inn på e-postkontoen.
- Ansatte får mulighet til å lese e-poster de ikke skulle sett fordi andre ansatte med tilgang til barnehagens e-postkonto har glemte å logge ut.

Eksempler på sikkerhetstiltak for å unngå uønskede hendelser

- Etabler rutiner for hvilke beskjeder og opplysninger som kan sendes per e-post, og hvem som skal ha mulighet til å gjøre dette.
- Ha retningslinjer for hvilken jobberelatert informasjon ansatte kan sende til eller fra private e-postadresser.
- Etabler rutiner for alternative kommunikasjonsløsninger dersom bruk av e-post blir utilgjengelig over lengre tid.
- Unngå å oppgi sensitive opplysninger i e-poster dersom ekstra sikringstiltak (kryptering) ikke benyttes.
- Sørg for at ansatte ikke logges automatisk inn på e-postkontoer hvis det benyttes felles datamaskin i barnehagen, og sørg for at det logges ut etter bruk.



TEKSTMELDINGER

Tekstmeldinger er et effektivt kommunikasjonsmedium som gjør det enkelt for foreldre eller ansatte i barnehagen å sende korte beskjeder. Tekstmeldinger kan deles inn i to grupper. Den ene er masseutsendelser, gjerne fra et administrativt system. Disse tekstmeldingene inneholder ofte generell informasjon fra barnehagen om turplaner, arrangementer og lignende. Den andre gruppen er individuelle meldinger som omhandler hvert enkelt barn. De kan for eksempel inneholde informasjon om at barnet blir hjemme fra barnehagen på grunn av sykdom, eller en bekreftelse fra barnehagen om at barnet har det bra etter en litt vanskelig levering på morgenen.

Med tanke på informasjonssikkerheten er det de individuelle meldingene som medfører størst risiko, da disse i større grad inneholder personopplysninger. Det kan dermed oppstå en rekke uønskede hendelser knyttet til denne typen tekstmeldinger.

Eksempler på uønskede hendelser som kan forekomme ved bruk av tekstmeldinger

- Uvedkommende leser en melding fordi den er sendt til feil telefonnummer.
- Uvedkommende får tilgang til sensitiv informasjon fordi ansatte benytter sin private telefon i jobbsammenheng og lar andre benytte den utenfor arbeidstid.
- Viktige beskjeder når ikke frem til riktig mottaker fordi telefonlister ikke er oppdatert.
- Mobiltelefonen har ikke aktivert automatisk lås med kode, noe som medfører at uvedkommende med tilgang til telefonen kan lese, sende eller endre tekstmeldinger.

- Mobiltelefonen blir stjålet slik at alt innhold blir tilgjengelig for uvedkommende.
- Foreldre eller ansatte i barnehagen sender uklare beskjeder via tekstmeldinger slik at mottakeren misforstår informasjonen.

Eksempler på sikkerhetstiltak for å unngå uønskede hendelser

- Etabler klare rutiner og regler for hva slags informasjon som kan sendes som tekstmelding.
- Sørg for at innholdet på mobiltelefonen(e) kan slettes på avstand hvis telefonen(e) mistes eller blir stjålet.
- Påse at informasjon på mobiltelefoner som ikke lenger er i bruk blir slettet på tilfredsstillende måte.
- Bruk et klart og tydelig språk i tekstmeldingene slik at informasjonen ikke kan feiltolkes.
- Etabler rutiner for hvordan telefonlister skal oppdateres og hvem som skal ha tillatelse til å gjøre dette.
- Sikre tjenestetelefoner og private mobiltelefoner som benyttes i jobbsammenheng på tilfredsstillende vis, for eksempel med en automatisk lås med kode som aktiveres etter kort tid.

**Visste du at
nordmenn sender
rundt 6 500 000 000
tekstmeldinger i året?**





ARKIVSKAP

I barnehagen er det svært vanlig med bruk av arkivskap for oppbevaring av papirdokumenter som inneholder sensitiv informasjon og personopplysninger. Hele 9 av 10 barnehager benytter dette for å sikre sine dokumenter. Papirdokumentene kan inneholde opplysninger som fødselsnummer, telefonnummer, nasjonalitet og adresse. I tillegg kan det være lagret opplysninger fra hjelpeinstanser som barnevern, PPT, helsestasjon og fagsentre i arkivskapet. For enkelte barn, spesielt de som har særskilte behov, kan det dreie seg om en stor mengde informasjon.

Papirdokumenter krever andre typer sikringstiltak enn elektronisk lagrede dokumenter, selv om prinsippene i stor grad ofte blir de samme. Dette er det viktig å være klar over for å unngå uønskede hendelser.

Eksempler på uønskede hendelser som kan forekomme ved bruk av arkivskap

- Uvedkommende får tilgang til dokumenter fordi arkivskapet står ulåst og uten tilsyn over lengre tid, eller fordi nøkkelen er lett tilgjengelig.
- Uvedkommende får tilgang til dokumenter fordi dokumentene ikke blir lagt tilbake i arkivskapet etter bruk.
- Arkivet inneholder flere versjoner av samme dokument, noe som kan resultere i at ansatte blir feilinformert fordi de ser på feil versjon av dokumentet.

- Dokumenter som skulle vært arkivert havner på avveie fordi de blir skrevet ut og ikke hentet fra skriveren.
- Dokumenter blir arkivert på feil sted og blir dermed vanskelige å finne igjen.
- Dokumenter blir ødelagt fordi arkivskapet er plassert i et rom som er spesielt utsatt for vannskader, eller er mangelfullt sikret mot brannskader.

Eksempler på sikkerhetstiltak for å unngå uønskede hendelser

- Ha klare rutiner for hva som skal arkiveres i arkivskapet, og hvordan dokumentene skal lagres (arkivplan).
- Dersom det er mulig, begrense antall personer som har tilgang til arkivskapet.
- Påse at arkivskapet alltid blir låst etter at dokumenter har blitt tatt ut eller lagt tilbake.
- Makuler dokumenter som ikke trenger å være i arkivskapet.
- Etabler et system for versjonshåndtering. Versjoner som ikke er arkivpliktige bør makuleres.
- Påse at dokumenter alltid arkiveres på riktig sted.

Visste du at politiattesten umiddelbart skal makuleres etter å ha være benyttet i en ansettelsessak?



ELEKTRONISK LAGRING

I barnehager lagres en rekke opplysninger elektronisk. Elektronisk lagring betyr at dokumenter og andre filer blir lagret på datamaskiner, servere eller eksterne lagringsenheter. Eksempler på filer kan være maler til ulike skjemaer, notater eller møtereferater. I tillegg forekommer det at papirdokumenter skannes og lagres elektronisk.

Fordelen med elektronisk lagring er at det ofte gir god sporbarhet. I tillegg åpner det for å lagre store mengder informasjon som lett kan flyttes. Nettopp disse forholdene gjør at sannsynligheten for og konsekvensene av uønskede hendelser kan bli store.

Eksempler på uønskede hendelser som kan forekomme ved bruk av elektronisk arkivering

- Uvedkommende får tilgang til informasjon lagret på en datamaskin fordi det er mulig å logge seg på uten bruk av passord.
- Uvedkommende har kjennskap til passordet til datamaskinen og kan dermed få tilgang til informasjonen.
- Det oppstår uklarhet rundt hvilken versjon av et dokument som er korrekt fordi flere ansatte har tilgang til å lagre eller gjøre endringer i dokumentene.
- Informasjon blir utilgjengelig fordi den bevisst eller ubevisst blir slettet.
- Viktig informasjon er ikke tilgjengelig ved behov fordi informasjonen er lagret på et område som de ansatte ikke har tilgang til.

- Ansatte får ikke tilgang til elektronisk lagret informasjon fordi datamaskinen eller datanettverket ikke er tilgjengelig.

Eksempler på sikkerhetstiltak for å unngå uønskede hendelser

- Ha klare rutiner for hvor og hvordan elektronisk informasjon skal lagres.
- Ha rutiner for sikkerhetskopiering slik at informasjonen kan gjenskapes dersom den skulle bli skadet eller utilgjengelig.
- Mest mulig informasjon bør lagres på en server fremfor lokalt på datamaskiner, da en server ofte er bedre sikret enn datamaskiner.
- Ha rutiner for hvordan elektronisk informasjonen skal oppdateres og endres.
- Begrens tilgangen til informasjonen og begrens antallet personer med mulighet til å endre på informasjonen.
- Sørg for at sensitiv informasjon er lagret på områder hvor det kreves passord for å få tilgang.
- Papirdokumenter bør makuleres etter at de er skannet slik at barnehagen ikke ender opp med dobbeltkopier.
- Sikre at nettverket er robust og driftssikkert slik at informasjon er tilgjengelig ved behov.

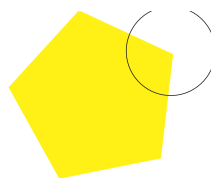
Er barnehagens minnepinner med sensitiv informasjon sikret?

MINNEPINNER

Minnepinner har blitt svært populære å bruke fordi de er små, enkle, robuste og billige. Muligheten for å lagre store mengder data gjør dem praktiske når det gjelder å flytte bilder og dokumenter mellom datamaskiner. Den fysiske størrelsen er derimot relativt liten, noe som gjør dem veldig mobile og lett å miste. Det er derfor viktig å ha et bevisst forhold til hvordan minnepinner skal håndteres for å unngå uønskede hendelser.

Eksempler på uønskede hendelser som kan forekomme ved bruk av minnepinner

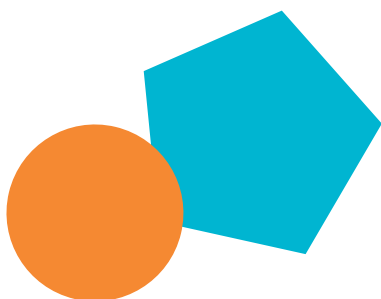
- En minnepinne mistes eller blir liggende tilgjengelig slik at opplysninger kommer uvedkommende i hende.
- Det oppstår tvil om hvilken versjon som er korrekt fordi informasjon som er lagret både på minnepinnen og datamaskinen ikke oppdateres på tvers av lagringsenhetene.
- Ansatte benytter private minnepinner, som inneholder datavirus eller annen uønsket programvare, slik at informasjon som er lagret på barnehagens datamaskiner skades.
- Informasjon blir tilgjengelig for uvedkommende fordi ansatte lagrer dokumenter på minnepinner og overfører dem til sin private datamaskin.



- Informasjon som ikke skulle vært kjent for alle blir tilgjengelig for uvedkommende fordi minnepinner blir delt blant flere ansatte.
- Viktig informasjon blir utilgjengelig fordi passordet til en minnepinne blir glemt.

Eksempler på sikkerhetstiltak for å unngå uønskede hendelser

- Etabler klare rutiner for hvordan minnepinner skal håndteres og hva slags informasjon som kan lagres på minnepinner.
- Ha systemer for merking og oppbevaring av minnepinner, spesielt hvis disse inneholder sensitiv informasjon.
- Vær bevisst på at minnepinner som deles av flere ansatte ikke inneholder annen informasjon enn den som skal deles.
- Påse at minnepinner med sensitiv informasjon er kryptert.
- Innfør sperre mot bruk av private minnepinner på barnehagens datamaskiner.
- Lag systemer som sikrer at passord som benyttes for sikring av minnepinner ikke blir glemt.



Når ryddet du sist i tilgangene til fjernarbeidsløsningen? Har tidligere ansatte fortsatt tilgang?



FJERNARBEIDSLØSNINGER

At ansatte ønsker å utføre arbeidsoppgaver fra en datamaskin de har hjemme kan være en fordel for både de ansatte og barnehagen. Det kan gi de ansatte større fleksibilitet i hverdagen ved at de selv kan styre når de vil fullføre møterefater, pedagogiske planer, arbeidsplaner og lignende.

Det er imidlertid viktig å være klar over at det også knytter seg en sikkerhetsutfordring til denne løsningen. Spesielt stor er risikoen dersom dokumenter med sensitiv informasjon flyttes ut av barnehagens kontroll. For å unngå uønskede hendelser er det derfor viktig å ha et bevisst forhold til hva det skal være lov til å jobbe med hjemmefra.

Eksempler på uønskede hendelser som kan forekomme ved bruk av datamaskin hjemme

- Familiemedlemmer får tilgang til sensitiv informasjon fordi den har blitt lagret på den ansattes private datamaskin.
- Familiemedlemmer får tilgang til sensitiv informasjon fordi den ansatte har glemt å logge seg ut fra fjernarbeidsløsningen.
- Skadelig programvare spres til barnehagens nettverk på grunn av manglende antivirusprogram på den ansattes private datamaskin.

Eksempler på sikkerhetstiltak for å unngå uønskede hendelser

- Etabler regler for hvilken type informasjon de ansatte har lov til å arbeide med hjemmefra.
- Reduser bruken av private datamaskiner ved å tilby bærbare datamaskiner som kun benyttes i jobbsammenheng.
- Dersom bærbare datamaskiner inneholder sensitiv informasjon bør de sikres ved bruk av kryptering.
- Etabler fjernarbeidsløsninger som gjør at de ansatte slipper å lagre informasjon lokalt på sin private datamaskin.
- Etabler fjernarbeidsløsninger som forhindrer at sensitiv informasjon kan hentes ut fra serveren.
- Sikre påloggingen til fjernarbeidsløsningen ved hjelp av engangspassord, som den ansatte for eksempel kan få tilgang til via en kodebrikke, tilsendt på mobil eller benytte smartkort.
- Tilgang via fjernarbeidsløsninger bør tidsbegrenses, og brukerne bør kobles fra automatisk hvis tilkoblingen har vært inaktiv i en viss tid.

Kontrolleres alltid samtykke fra foreldrene før bilder av barna distribueres eller publiseres?

FOTO OG VIDEO

Bruk av digitale kameraer og annet fotoutstyr er en vanlig aktivitet i barnehager. Det tas bilder av både barn og ansatte på turer, under bursdagsfeiringer, i forbindelse med pedagogiske aktiviteter, eller i andre hverdagssituasjoner. Digitale kameraer har gjort det enkelt å overføre eller kopiere bilder til annet digitalt utstyr. Dette gir en rekke muligheter, for eksempel bruke bildene i aktiviteter sammen med barna, distribuere bildene rundt, eller publisere dem på nettet. Det samme gjelder for øvrig både lyd og video som tas opp i barnehagen.

Bruk av foto- og videoutstyr medfører en rekke utfordringer. Bevissthet og kritisk refleksjon omkring bruk av foto og video i barnehagesammenheng er derfor viktig for å unngå uønskede hendelser.

Eksempler på uønskede hendelser som kan forekomme ved bruk av foto og video

- Ansatte mister barnehagens kamera, minnekort eller andre lagringsmedier, slik at filene blir tilgjengelige for uvedkommende.
- Det blir filmet eller tatt bilder av barna uten at det er innhentet samtykke fra foreldrene.
- Uvedkommende får tilgang til bilder tatt i barnehagen fordi ansatte benytter sitt private kamera eller sin private mobiltelefon i jobbsammenheng.
- Bilder blir sendt til feil mottaker ved bruk av e-post eller mobiltelefon.



- Bilder som lagres på private datamaskiner eller skytjenester havner på avveie og blir gjort tilgjengelige for uvedkommende.
- Barnehagen mister tilgang til bilder fordi tidligere ansatte har lagret disse på sin private datamaskin.
- Barnehagen mister tilgang til bilder fordi leverandøren av en ekstern lagringsløsning går konkurs eller sletter bildene.

Eksempler på sikkerhetstiltak for å unngå uønskede hendelser

- Ha retningslinjer og rutiner for hvordan bruk av utstyr skal foregå, og hvordan fotograferingen og bildene skal håndteres.
- Minnekort bør slettes etter at bilder er overført til datamaskin eller annet lagringsmedium.
- Ha rutiner for kontroll av samtykke fra foreldrene ved fotografering eller filming av barna.
- Ha rutiner for gjennomgang av kontaktinformasjon dersom bilder skal sendes til foreldre per e-post eller mobiltelefon.
- Ha klare regler for bruk av private utstyr som benyttes til å ta bilder og video i jobbsammenheng.

Er informasjonen på barnehagens hjemmeside godt nok sikret?



HJEMMESIDER

I dag har nærmere åtti prosent av barnehagene sin egen hjemmeside. Noen drifter den selv mens andre er tilknyttet kommunens eller eierens nettsted. Hva slags innhold som legges ut på hjemmesiden varierer fra barnehage til barnehage. De fleste legger ut barnehagens kontaktinformasjon, informasjon om opptak, lovverk, årsplan, eller andre nyttige opplysninger. Noen legger også ut bilder, tegninger, animasjonsfilmer og andre ting som barna har laget.

Har barnehagen hjemmeside er det viktig å ha kjennskap til hvilke uønskede hendelser som kan oppstå og hvilke sikkerhets tiltak som kan iverksettes.

Eksempler på uønskede hendelser som kan forekomme ved bruk av hjemmesider

- Foreldre blir feilinformert fordi det publiserte innholdet på hjemmesiden ikke er korrekt.
- Det publiseres personopplysninger på hjemmesiden som ikke skulle vært kjent for uvedkommende.
- Uvedkommende får tilgang til passordbeskyttet innhold på hjemmesiden fordi foreldre eller ansatte benytter felles passord ved pålogging.
- Uvedkommende får tilgang til bilder av barn som foreldrene ikke har gitt samtykke til å publisere på hjemmesiden.

- Foreldre får ikke tilgang til viktig informasjon fordi hjemmesiden ikke er tilgjengelig.
- Hjemmesiden blir hacket og benyttet til å spre virus og skadelig programvare.

Eksempler på sikkerhetstiltak for å unngå uønskede hendelser

- Ha rutiner for hva slags informasjon som skal være tilgjengelig på hjemmesiden, hvordan informasjonen skal oppdateres, og hvem som skal ha adgang til å utføre endringer.
- Benytt et passordbeskyttet område til å publisere informasjon som ikke skal være tilgjengelig for uvedkommende.
- Sikkerhetsinnstillinger for hjemmesiden bør administreres av personer som har kompetanse på dette.
- Sørg alltid for at det finnes en sikkerhetskopi av hjemmesiden, slik at den kan rekonstrueres hvis det skulle oppstå problemer.
- Sørg for at informasjonen som publiseres på hjemmesiden er fullstendig og oppdatert, samt i tråd med foreldrenes ønsker og barnehagens retningslinjer.

SOSIALE MEDIER

Bruken av sosiale medier blant befolkningen har økt de siste årene, og omtrent 15 prosent av barnehagene benytter nå slike medier. Det er stadig flere foreldre som etterlyser at barnehagen benytter sosiale medier og det kan derfor tenkes at dette er noe som vil øke i omfang i fremtiden. Ansatte i barnehagene er på den annen side skeptiske til dette. De mest brukte sosiale mediene i barnehager er Facebook, Twitter, Youtube og ulike bloggsider.

Fordelen med sosiale medier er at det er lett å dele informasjon med mange. Ulempen er at det kan være vanskelig å kontrollere hva slags informasjon som blir delt og hvem som får tilgang til den.

Eksempler på uønskede hendelser som kan forekomme ved bruk av sosiale medier

- Ansatte i barnehagen benytter sosiale medier til å spre informasjon som er taushetsbelagt.
- Uvedkommende får tilgang til bilder av, og informasjon om, barn i barnehagen som ansatte har publisert på sosiale medier uten samtykke fra foreldrene.
- Ansatte utgir seg for å representere barnehagen i offentlige debatter på nettet og gir uttrykk for holdninger som ikke er i tråd med barnehagens verdier.
- Ansatte benytter sosiale medier til å publisere informasjon som kun burde vært publisert på barnehagens hjemmesider.



Eksempler på sikkerhetstiltak for å unngå uønskede hendelser

- Etabler klare retningslinjer for hvordan barnehagen ønsker å benytte sosiale medier, for eksempel hva slags informasjon som kan publiseres og hvem som har adgang til å gjøre dette.
- Tenk gjennom og bli bevisst på risikoen ved bruk av sosiale medier. Informer også ansatte om dette.
- Vær tydelig på, og ha en felles forståelse av, hvor grensen mellom jobberelatert og privat bruk av sosiale medier går.

SKYTJENESTER

Skytjenester har de siste årene vokst frem som et alternativ til den tradisjonelle måten å drifte og organisere IT på. I barnehagen er det foreløpig vanligst å benytte seg av programtjenester som Dropbox, Google Drive, SkyDrive og iCloud. Bruken av slike programtjenester åpner for å lagre og dele bilder og dokumenter "i skyen". Fordelene med denne løsningen er at dokumentene automatisk kan synkroniseres til flere enheter (datamaskiner, nettbrett, eller smarttelefoner) og at det tas en sikkerhetskopi av filene. Skytjenestene kan brukes både til lukkede grupper, hvor kun de ansatte har tilgang til informasjon, og til mer åpne grupper hvor barnehagen kan dele bilder og informasjon med foreldrene.

Utfordringene ved bruken av disse tjenestene knytter seg til å bevare kontrollen over hvem som kan se og endre informasjon, og hva slags informasjon som er delt.

Eksempler på uønskede hendelser som kan forekomme ved bruk av skytjenester

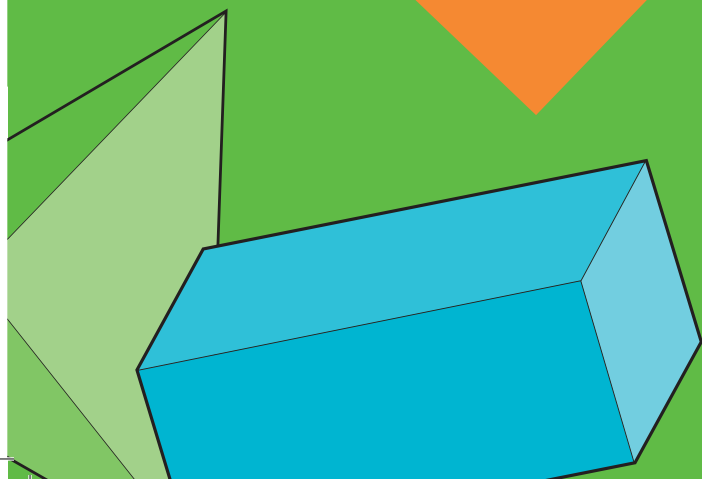
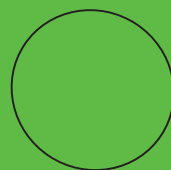
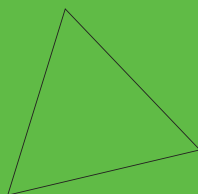
- Uvedkommende får tilgang til sensitiv informasjon fordi kontrollrutinene for hvem som har tilgang til delt informasjon ikke er gode nok.
- Barnehagen tar i bruk skytjenester uten at det foreligger en databehandleravtale med leverandøren.
- Uvedkommende får tilgang til personopplysninger fordi ansatte har synkronisert skytjenestekontoen med private enheter.
- Viktig informasjon blir feilaktig fordi mange ansatte har mulighet til å gjøre endringer på informasjonen som er lagret i skyen.
- Informasjonen i skyen blir utilgjengelig fordi leverandøren legger ned tjenesten uten å melde fra om dette.

Eksempler på sikkerhetstiltak for å unngå uønskede hendelser

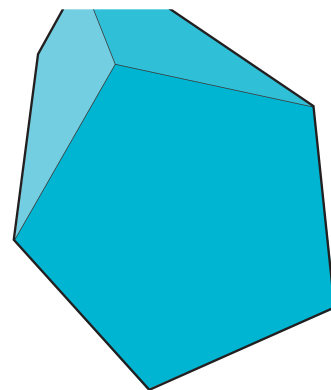
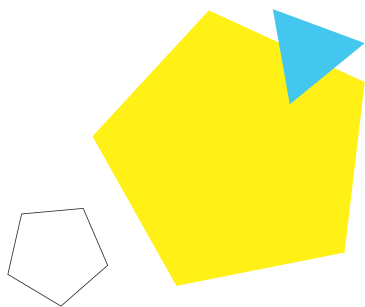
- Etabler klare rutiner for hva slags informasjon som kan lagres i skyen og hvem som skal ha tilgang til informasjonen.
- Påse at det foreligger en databehandleravtale når skytjenester tas i bruk.
- Benytt personer med kompetanse på skytjenester ved valg av leverandør.
- Begrens antallet dataenheter som er synkronisert mot skytjenestekontoen.



**Visste du at over
2 500 000 nordmenn
har en konto på Facebook?**

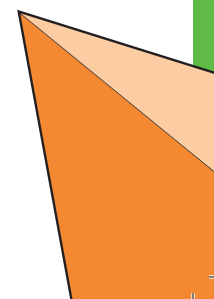
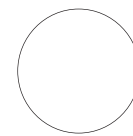


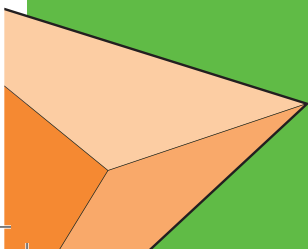
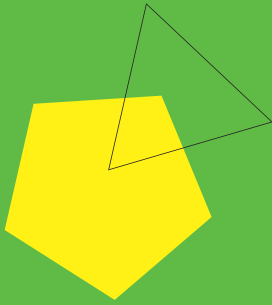
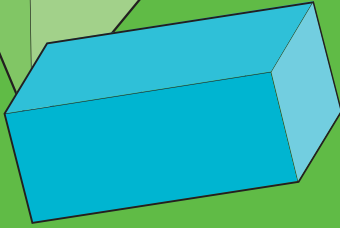




Ordliste

- Administrativt system:** Et system som benyttes i den daglige driften av barnehagen. Kan omfatte alt fra behandling av barnehagesøknader, utsending av brev, fakturering, regnskap til støtte av utarbeidelse av rapporter.
- Arkivplan:** En ajourført samleplan som viser hva arkivet omfatter og hvordan det er organisert. Arkivplanen viser også hvilke instruksjoner og regler som gjelder for arkivarbeidet.
- Databehandleravtale:** En avtale som må inngås dersom behandling av personopplysninger settes ut til eksterne virksomheter, såkalte databehandlere. Dette kan være en egen avtale mellom partene eller inngå som en del av et annet avtaleverk. Les mer her: http://www.datatilsynet.no/Global/04_veiledere/Databehandleravtaler_20090526.pdf
- Digitale verktøy:** Verktøy som benyttes som digitale hjelpemidler, for eksempel datamaskiner, nettbrett, mobiltelefoner, digitale fotoapparater og digitale videokameraer.
- Eksternt skrivebord:** En løsning som gjør det mulig å opprette en ekstern forbindelse til en datamaskin eller servere lokalisert andre steder. All behandling av dokumenter vil skje lokalt på datamaskinen eller serveren det er opprettet en ekstern forbindelse til.
- Engangspassord:** Et passord som benyttes bare én gang. Bruk av engangspassord øker dermed sikkerheten ved pålogging til en fjernarbeidsløsning. Passordet kan for eksempel genereres ved hjelp av en kodebrikke, en tekstmelding, en mobilapplikasjon, eller et smartkort. Ved pålogging benyttes dette i tillegg til den ansattes faste påloggingspassord.
- Fjernarbeidsløsning:** En løsning som gjør det mulig å opprette en ekstern forbindelse til en datamaskin eller servere lokalisert andre steder. Løsningen kan innebære bruk av eksternt skrivebord, men brukeren kan også få mulighet til å behandle dokumenter lokalt på sin datamaskin.
- Informasjonssikkerhet:** Handler om at informasjon sikres med hensyn til konfidensialitet, integritet og tilgjengelighet.
- Integritet:** Betegnelse på at informasjon er korrekt og foreligger i original form uten å vært utsatt for uautoriserte endringer.
- Konfidensialitet:** Dreier seg om å sikre at informasjon ikke avsløres for uvedkommende.
- Kryptering:** Har sammenheng med ordet kryptografi, som betyr "skjult tekst". Kryptert informasjon blir gjort uleselig for uvedkommende.
- Personopplysninger:** Opplysninger og vurderinger som direkte og indirekte kan knyttes til en enkeltperson.
- Server:** Maskinvare og programvare som muliggjør deling av informasjon og programmer mellom flere datamaskiner tilknyttet et nettverk.
- Tilgjengelighet:** Innebærer at informasjon skal være tilgjengelig for de rette vedkommende ved behov.





**SENTER
FOR IKT I
UTDANNINGEN**

www.iktsenteret.no

