**INNHOLDSFORTEGELSE**

1. **FORORD**
2. **PERSONOPPLYSNNGER**
3. **HVA DU SKAL VÆRE KJENT MED**
4. **ROLLER OG ANSVARSFORDELING**
5. **RETNINGSLINJER FOR INFORMASJONSSIKKERHET** 
   1. **MÅL FOR INFORMASJONSSIKKERHET**
   2. **SIKKERHETSTILTAK DU ER PÅLAGT Å KJENNE TIL OG ETTERLEVE I DET DAGLIGE**
6. **RUTINER FOR AVVIKSHÅNDTERING OG EGENKONTROLL**
7. **SANKSJONER VED BRUDD PÅ RETNINGSLINJER**
8. **VEDLEGG**
9. **LITTERTURLISTE**
10. **FORORD**

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 retningslinjene er å hjelpe barnehagepersonalet til å oppfylle sine lovpå­lagte plikter og sikre at personopplysningene blir håndtert på en forsvarlig måte.

Retningslinjene er utarbeidet i tråd med gjeldende lovverk, veilederen «Informasjonssikkerhet i barnehagen» (Senter for IKT i barnehagen) og ”lærerprofesjonens etiske plattform”.

1. **PERSONOPPLYSNINGER**

I personopplysningsloven skilles 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

**3. HVA DU SKAL VÆRE KJENT MED:**

* ROLLER OG ANSVARSFORDELING
* RETNINGSLINJER FOR INFORMASJONSSIKKERHET
* RUTINER FOR AVVIKSHÅNDTERING OG EGENKONTROLL.
* SANKSJONER VED BRUDD PÅ RETNINGSLINJER
* VEDLEGG

1. **ROLLER OG ANSVARSFORDELING**

Barnehagens medarbeidere skal bare bruke informasjonssystemene for å utføre pålagte oppgaver, og de skal autoriseres for tilgang etter barnehagens rutiner.   
Alle medarbeiderne skal ha nødvendige kunnskaper for å bruke systemene i samsvar med fastlagte rutiner. Tilgang gis ved tiltredelse samtidig som umiddelbar og fortløpende opplæring finner sted. Alle har et viktig ansvar for å melde avvik i tråd med barnehagens rutiner for avvikshåndtering

Personvernlovgivningen angir roller, ansvars- og myndighetsområde i et internkontroll/-HMS-system:

**Eier** og styrer utgjør barnehagens sikkerhetsutvalg, et overordnet styringsorgan for oppfølging av personvernlovgivningens krav om informasjonssikkerhet.

**Styrer** har det overordnede ansvar for at personopplysninger barnehagen behandler er tilfredsstillende sikret. Styrer er den som koordinerer sikkerhetsarbeidet gjennom opplæring, oppfølging og kvalitetssikring av retningslinjer og rutiner.   
Styrer/ HMS-ansvarlig har ansvar for opplæring, vedlikehold av og ajourhold av tilganger/passord. Det må ved lengre tids fravær og avslutning av arbeidsforhold sikres at tilganger opphører. Det er styrer du skal henvende deg til dersom du har behov for mer opplæring i informasjonssystemet.

**Daglig ansvarlig**Det daglige ansvaret ved behandling av personopplysninger er delegert til den aktuelle bruker. Det betyr et delegert daglig ansvar til pedagogiske ledere, fagarbeidere, assistenter og vikarer for å påse at sikkerheten er ivaretatt.

**Verneombudet** skal påse at arbeidstakers rettigheter og plikter følges opp.

1. **RETNINGSLINJER FOR INFORMASJONSSIKKERHET** 
   1. **MÅL FOR INFORMASJONSSIKKERHET**

* Alle ansatte og brukere skal være trygg på at sensitiv informasjon ikke kommer på avveie.
* Alle ansatte skal aktivt sette seg inn i og kjenne til barnehagens mål for sikkerhet og retningslinjer for å sikre personvernet og sørge for sikker informasjonsbehandling.

**5.2 SIKKERHETSTILTAK DU ER PÅLAGT Å KJENNE TIL OG ETTERLEVE I DET DAGLIGE**

**Regler for taushetsplikt**

Alle har taushetsplikt i tjenestesaker. Denne bestemmelsen skal hindre at informasjon som kan spores tilbake til en person, gjøres kjent for uvedkommende. Dette gjelder opplysninger om brukere, ansatte og barnehagens virksomhet, både i muntlig, skriftlig og elektronisk format.

Taushetsplikten gjelder ikke bare utad, men *også* overfor andre medarbeidere og kollegaer der opplysningene må anses unødvendige. Taushetsplikten gjelder også etter at arbeidsforholdet er avsluttet, og varer i praksis livet ut.

Ingen medarbeider skal aktivt søke konfidensielle eller sensitive opplysninger når de ikke er nødvendige for den ansattes arbeid i barnehagen.

**Orden og ryddighet på kontor**

* Alle medarbeidere er ansvarlig for at personopplysninger på egen arbeidsplass er forsvarlig sikret.
* Saksdokumenter skal ikke ligge åpent uten tilsyn.
* Dokumenter skal låses inn før arbeidsdagens slutt.
* Datamaskiner skal logges av før arbeidsplassen forlates.
* Alle datamaskiner skal ha aktivert skjermsparer slik at kode må skrives inn..
* Kontor skal låses ved dagens slutt/ ved arrangement

**Arkiv**Fysisk sikring av personopplysninger er et svært viktig tiltak for å hindre at uvedkommende får tilgang til opplysningene.

* Fast ansatte og ansatte i vikariat har tilgang på arkivet. Andre skal kontakte styrer for innsyn i arkiv.
* Arkivet skal til enhver tid være ryddig og oversiktlig slik at bruker kan se innhold i sin mappe.
* Interne notater kan gi unntak fra innsynsrett hvis tekst er utarbeidet for intern saksforberedelse og ikke utlevert til andre (se vedlegg).
* Arkivet skal være låst når kontoret ikke er besatt.
* Avdelingsbøker og notatbøker skal låses ned ved arrangement i barnehagen.
* Papirer med personopplysninger skal ikke tas med hjem.
* Kod det som skrives hjemme i ubunden tid.
* Makuler info når ny info legges i mapper.
* Registrer post før arkivering.

**Regler for bruk av e-post**

* Bedriftens e-post skal åpnes hver dag.
* E-postadresser bør ha navn som relaterer til bedriften.
* Aldri legg inn automatisk passord.
* Mobil **skal** ha kode hvis denne brukes til jobb-mail.
* E-post må ikke benyttes til å sende konfidensiell / personsensitiv informasjon.
* Dersom ansatte mottar e-post som inneholder konfidensiell / personsensitiv informasjon, er de ansvarlig for å gjøre avsender oppmerksom på at de ikke kan svare på e-post av denne type. Styrer plikter å gjøre oppmerksom på at henvendelser må skje per telefon eller brev.
* Sikre rett mottaker før du trykker ”send”.
* Husk at en ikke har noen garanti for at meldingen når mottakeren, sjekk derfor opp at mottaker har mottatt informasjon.
* Arbeidsgiver kan, i spesielle tilfeller og ved saklig behov, lese ansattes virksomhets-relaterte  
   e-post.
* Benytt alltid emnefelt (subjekt).
* Det skal ikke sendes ut Spam, som er utsending av en ensartet melding til et stort antall mottakere, som på forhånd ikke har sagt seg villig til å motta e-posten.
* Annonsering o.l. er ikke tillatt.
* Kjedebrev eller virusadvarsler skal ikke videresendes.
* Den som åpner posten har plikt til å vurdere om e-posten skal anses som et arkivverdig dokument. E-post som skrives ut vil da være arkiveksemplaret av dokumentet. Vær obs på at selv om personlige eller private kommentarer er blandet inn i teksten, kan e-posten være et saksdokument.
* Det gis åpning for begrenset privat bruk av barnehagens e-post såfremt dette ikke innebærer økt risiko og barnehagens retningslinjer følges.
* Filer skal kontrolleres for virus før de åpnes.

**Sosiale medier** (facbook, twitter, youtube, blogg med mer)

* Bland aldri jobb og privatliv. Husk at foreldre/brukere anser deg som ansatt i barnehagen 24/7.
* Legg aldri ut info om barnehagen eller brukere.
* Understrek at du uttaler deg som privatperson.
* Tenk nøye gjennom konsekvenser før du legger ut informasjon eller bilder på sosiale medier.

**Hjemmesider /aviser**

* Tilgang til administrasjonssider og ansvar for info skal avklares med styrer.
* Informasjon som legges på hjemmeside og aviser skal være generell og ikke inneholde personlige opplysninger.
* Skriftlig samtykke fra foreldre skal foreligge før bilder distribueres.
* Bilder av enkeltbarn/ nærbilder skal kun legges på kodete foreldresider.
* Bilder som distribueres til ”alle” skal være gruppebilder el bilder av aktiviteter, ikke nærbilder som kan misbrukes.
* Hjemmesider må sikkerhetskopieres.

**Bærbare datamaskiner tilhørende barnehagen**

* Maskinen skal kun benyttes av deg som ansatt, og ikke lånes ut til familiemedlemmer eller andre.
* PC`er med sensitiv informasjon skal ha kode.
* Det er ikke tillatt å installere, endre eller fjerne programmer og funksjonalitet på datamaskinen. Ved behov for slike endringer, skal styrer kontaktes.
* Ved feil på datautstyr, skal styrer kontaktes.

**Foto og videoutstyr**

* Foreldre skal samtykke til fotografering og filming, uansett henseende.
* Kun barnehagens utstyr skal brukes.
* Avklar formål og tidspunkt for sletting ved spesifikke oppdrag.
* Minnekort skal slettes når bilder er overført til pc, og når mål med film er oppnådd.

**Privat datautstyr og private mobiler**

* Sensitive opplysninger skal ikke lagres på privat pc/ mobil.
* Alle opplysninger og info på privat utstyr skal også lagres på barnehagens pc.
* Alle barnehagerelaterte dokumenter skal ha egen bruker hvis privat pc brukes av andre i heimen.
* Private mobiler og kamera skal ikke brukes til fotografering i barnehagen.

**Mobiltelefoner / tekstmeldinger**

* Foreldre skal ikke kontakte ansatte på fritid/ privat på mobil eller sosiale medier.
* Tlf og mail-lister skal til enhver tid være oppdatert for å unngå feilsending av sms.
* Jobb-tlf og private tlf som benyttes i jobb skal ha automatisk lås med kode som aktiveres etter kort tid.
* Sms med personlige opplysninger skal slettes når «samtale» er over.
* Sms`er skal ikke inneholde sensitive opplysninger.
* Info som sendes per sms skal være så tydelig at den ikke kan misforstås.
* Private mobiler skal kun benyttes i pauser. Annen bruk avtales med nærmeste overordnede.

**Ekstern harddisk og server**

* Mest mulig informasjon bør lagres på en server/ekstern hardisk fremfor lokalt på datamaskiner som sikkerhetskopi.
* Ekstern harddisk/ server skal ikke inneholde sensitive opplysninger.
* Server/harddisk sikrer tilgang til enhver tid for de som har behov for tilgang.
* Ekstern harddisk skal låses ned i arkiv.

**Skytjenester**

* 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.

**Bruk av minnepinner**

* Barnehagen skal holde minnepinner til de som har behov for det. Skal være merket med navn/rolle/ avdeling.
* Private minnepinner skal ikke brukes.
* Brukes minnepinne på maskiner utenom barnehagen skal denne skannes for virus.
* Minnepinne skal ikke brukes til personlige opplysninger hvis den skal tas ut av barnehagen.
* Minnepinne som inneholder personlige opplysninger skal låses ned i arkiv og bare brukes i barnehagen.
* Hvis flere ped.ledere bruker samme minnepinne skal den ikke inneholde personlige opplysninger.
* Minnepinne med sensitiv informasjon skal være kryptert.

**Bruk av passord**

* Passord er den viktigste måten å sikre opplysninger lagret i datasystem på.
* Det er ikke tiltatt å dele passord, og passordet ditt skal ikke skrives ned noen plass.
* Når ansatte slutter må passord endres for å fjerne tilgang til informasjon.

**Muntlig dialog**

Vær bevisstpå hvor du er når dusnakker om personopplysninger og sensitiv informasjon. Du vet aldri hvem som kan overhøre samtalen.

* Når du får informasjon fra foreldre..
* Når du skal overføre muntlig info må du sikre at ingen kan overhøre samtalen. Lukk evt. dør, og tenk over mulige ører utenfor synsvidde.
* Vit at den info du gir er faktabasert og ikke basert på rykter..

**Den registrertes rettigheter**Samtykke, rett til informasjon og det å kunne utøve innsynsrett er grunnleggende rettigheter i personvernlovgivningen. Ønsker om innsyn skal videreformidles til nærmeste leder.

**Ledere** skal kjenne til følgende prosedyrer:

* Regler for innhenting av samtykke (Se vedlegg)
* Regler for innsyn og informasjonsplikt (Se vedlegg)
* Regler for retting og sletting (Se vedlegg)

1. **RUTINER FOR AVVIKSHÅNDTERING OG EGENKONTROLL**

Arbeidsgiver skal gjennomføre egenkontroller for å forbedre kvaliteten og sikkerheten i informasjonsbehandlingen. Avviksbehandling skal iverksettes ved brudd på sikkerhetstiltak og/eller når oppgaver er utført i strid med de rutiner som er besluttet.

**Melding av avvik**

Alle medarbeidere er ansvarlig for å melde avvik ved å bruke vedlagte avviksskjema. Avvikene skal behandles av styrer eller nærmeste leder, og følges opp av berørte parter innen en gitt frist.

**Egenkontroll**

En viktig del i sikkerhetsarbeidet, er en jevnlig kontroll med hvordan sikkerhetstiltakene og internkontrollen (HMS) er kjent i barnehagen.

For å kontrollere sikkerhetsnivået gjennomføres egenkontroller via spørreskjema til alle ansatte. Styrer og den enkelte ansatte er ansvarlig for å følge opp evt. avvik.

Egenkontroll gjennomføres årlig i perioden januar – mars.

1. **SANKSJONER VED BRUDD PÅ RETNINGSLINJER**

Behandling av personopplysninger og bruk av datasystemer i strid med retningslinjene, personvernlovgivningen, forvaltningsloven og egne særlover anses som tjenesteforsømmelse.   
Det vil kunne føre til sanksjoner i henhold til barnehagens arbeidsreglement.

Arbeidsgiveren kan gi beskjed om at det vil bli kontrollert hvem som står for evt. ureglementerte aktiviteter dersom den ikke opphører innen en gitt frist. Dersom aktiviteten ikke er opphørt innen fristen, vil arbeidsgiveren, uten samtykke fra de ansatte, kunne gå inn i loggene.  
Ulovlig aktivitet med egen mobil eller pc vil kunne føre til anmeldelse.

1. **VEDLEGG:**
2. Kontrakt
3. Taushetserklæring
4. Avviksskjema
5. Regelverk for oppbevaring av personalmapper
6. Regelverk tilknyttet dokumentasjon og vurdering (barn)
7. Unntak fra retten til informasjon
8. Kontrollskjema
9. Lærerprofesjonens etiske plattform
10. **LITTERATURLISTE**

«I beste mening… Et veiledningshefte om bilder av barn på nett»  
Datatilsynet 2008  
[www.datatilsynet.no](http://www.datatilsynet.no)

«Informasjonssikkerhet i barnehagen. En veileder i håndtering av personopplysninger og viktig informasjon»  
Senter for IKT i utdanningen 2013,   
[www.iktsenteret.no](http://www.iktsenteret.no)

Lærerprofesjonens etiske plattform, Utdanningsforbundet 2012.  
www.utdanningsforbundet.no

Personopplysningsloven  
www.lovdata.no