Selvejende Institution

Retningslinjer for håndtering

og

beskyttelse af personoplysninger

MINE NOTER

Er du i tvivl om noget kan spørgsmål til håndtering og beskyttelse af personoplysninger besvares af

Marengsen

Udarbejdet af:	Karin Riis	Godkendt af ledergruppen:	ja
Revideret:	090224	Godkendt af MED:	ja

INDLEDNING

Følgende retningslinjer skal være med til at sikre, en ensartet håndtering af de personoplysninger vi hver dag behandler om borgere, medarbejdere og andre, samt at personoplysninger er tilstrækkeligt beskyttet.

Alle medarbejdere har ansvaret for, at retningslinjerne overholdes.

Hvis der er udpeget en konkret ansvarlig, fremgår det pr. punkt.

Spørgsmål til retningslinjerne skal rettes til Karin Riis, leder.

HVILKE PERSONOPLYSNINGER ARBEJDER VI MED

Vi arbejder med mange personoplysninger i dagligdagen som typisk er den almindelige personlige information om borgerne eller medarbejdere.

Ud over disse skal vi særligt være opmærksom på følgende oplysninger:

Fortrolige personoplysninger	Følsomme personoplysninger
Cpr-nummer	Etnicitet
Familieforhold	Helbred
Indkomstforhold	Seksuelle forhold
Kontooplysninger	Seksuel overbevisning
Sociale forhold	Fagforening (medarbejder)
Straffedomme / lovovertrædelser	

HÅNDTERING AF PERSONOPLSYNINGER

Personoplysninger:

- indsamles kun, hvis de er nødvendige for opgaveløsningen.
- bruges kun til de opgaver, der udføres indenfor vores ansvarsområde ved håndtering og pleje af beboere.
- må ikke deles med uvedkommende eller kunne overhøres af uvedkommende.
- skal være korrekte. Det vil sige, at oplysningerne skal være opdateret.
- skal opbevares, hvis det er nødvendigt, eller hvis det er et krav - øvrige oplysninger slettes.
- skal opbevares forsvarligt og må ikke være tilgængelige for uvedkommende, uanset om det er i systemer, i elektroniske filer, fysiske dokumenter, løse papirnoter mv. Adgangen til fortrolige og følsomme oplysninger skal være beskyttet af adgangskoder, nøgler etc.

Vi opbevarer hovedparten af personoplysninger i Aula ifm. vores sagsbehandling / dokumentation af børnenes sager.

Alle personoplysninger/informationer skal registreres i Aula hurtigst muligt. Papirdokumenter / Word-filer og andet der er brugt som grundlag skal derefter makuleres/slettes.

Vi opbevarer desuden personoplysninger på lokal PC ifm. daglig drift

Fx dagens opgaver, daglige driftsliste, medicinlister, allergilister, medarbejderoversigter, kontaktlister til forældre, billeder som vi har et formål med at gemme mv.

Der er oprettet mapper, hvor relevante medarbejdere har adgang svarende til afdeling, ansvar og opgaver.
Ansvarlig for mapper og adgange: Daglig leder

Nødvendige daglige drift- og opgavelister kan opbevares fysisk/synligt på kontor, hvis døren er låst.

Eventuelle særlige dokumenter, nødproceduremapper mv. med fortrolige og følsomme oplysninger opbevares i aflåste skabe.

Procesområde	Slettefrist	Sletning skal ske	Type af oplysninger			Slettemetode	Ansvarlig
			Alm	For.	Føl.		
Pladsadministration, daglig drift, underretning	1 år efter at barnet har forladt SI	December	x	x	x	Makulering af papirer Manuelt fra lokal enhed	
Samtykke-dokumenter (fysisk)	Så længe person-oplysning anvendes	December	x	x	x	Makulering af papirer	
Personale arbejdsskade	30 år efter sagen er afsluttet	December	x	x	x	Manuelt fra lokal enhed	
Personalesager ansæt. drift, fratræd	5 år efter sagen er afsluttet	Juni	x	x	x	Manuelt fra lokal enhed	
Daglig drift (økonomi) revision	5 år efter regn-skabsafslutning	Juni	x	x	x	Manuelt fra lokal enhed	
Administration Klagesag & indsigtsanmodninger	5 år efter endt sagsbehandling	Juni	x	x	x	Makulering af papirer Manuelt fra lokal enhed	
Personale – Ansøgninger	6 mdl. efter ansættelse	6 mdl. eft. ansøgningsfrist	x	x		Makulering af papirer Manuelt fra lokal enhed	
Administration - Arbejdsmiljø / klage	5 år efter at sagen er afsluttet	Juni	x	x	x	Manuelt fra lokal enhed	
Billeder / video / sociale medier	Må max være 3 mdl. gamle	Marts, Juni, Sept., Dec.	x			Makulering af papirer Manuelt fra lokal enhed System/Infoboard	Alle m. adgang
Mails / møde invitationer + papirkurv	Må max være 6 mdl. gamle	Juni og December	x	x	x	Manuelt fra lokal enhed	Alle m. adgang
Drifts- og arbejdslister	Løbende når behov er væk	Lige måneder	x	x		Makulering af papirer Manuelt fra lokal enhed	Alle m. adgang

FYSISK SIKKERHED, ADGANG TIL LOKALER MV.

Institutionen har åben adgang til en del lokaler, derfor skal medarbejdere løbende sikre, at dokumenter, lister og andet med personoplysninger håndteres forsvarligt i forhold til typen af oplysninger. Det vil bl.a. sige:

- Lister og dokumenter skal så vidt muligt skærmes, så de ikke kan ses af uvedkommende
- Kontorer/skabe skal låses, når de ikke benyttes.
- Skriveborde skal være ryddet for personoplysninger
- Gæster skal ikke have adgang til kontorer uden opsyn.
- Døre og vinduer holdes lukket udenfor normal arbejdstid

UDDANNELSE AF MEDARBEJDERE

Nye medarbejdere skal inden for den første måned efter ansættelse, have gennemlæst PIXI for medarbejdere og modtage introduktion til interne retningslinjer.

Alle medarbejdere skal hvert 2. år gennemgå GDPR uddannelse.

SLETTEREGLER

Generelle retningslinjer
Personoplysninger skal slettes, når der ikke er noget formål med eller krav til at opbevare oplysningerne mere.

Slettefrister skal overholdes uanset hvordan og hvorfor personoplysninger opbevares. Fx i it-systemer / Teams, i mails, på USB-stik, mobiltelefoner, IPads og tilsvarende mobile enheder, fysiske dokumenter i aflåste arkivskabe etc.

En slettefrist er det tidspunkt hvor den praktiske sletning skal finde sted.

Herunder fremgår slettefrister og tidspunkt og ansvarlige.

KOMMUNIKATION MED BORGER OG PÅRØRENDE

Skriftlig og mundtlig kommunikation skal ske, så uvedkommende ikke ser/hører om personoplysningerne.
Når kommunikationen indeholder fortrolige eller følsomme personoplysninger, skal der være en særlig opmærksomhed.

E-mail med fortrolige eller følsomme personoplysninger skal sendes krypteret ved hjælp af "Send sikkert" funktionen på e-mail, eller sendes som digital post.

Borgere, pårørende eller andre kan ikke give tilladelse til, at der sendes fortrolige eller følsomme oplysninger fx via usikker mail.

Inden en mail afsendes, skal det kontrolleres, at modtager er korrekt. Sendes e-mail til en forkert modtager, anmeldes dette som persondatabrud til leder.

Chat-funktioner på Facebook og SMS må ikke anvendes til kommunikation.

OPLYSNINGSPLIGT – om de personoplysninger vi bruger

Vi har en oplysningspligt, som betyder at forældre, pårørende mv. skal oplyses om, hvilke personoplysninger vi behandler om børnene og forældre mv. og på hvilket grundlag vi gør dette.

De pågældende modtager derfor vore privatlivspolitik og information om, hvor de kan genfinde denne.

HENVENDELSER - fra borgere, pårørende mv.

Vi har en pligt til at besvare henvendelser fra borgere, pårørende mv. om deres personoplysninger.

Hvis en borger, pårørende eller andre, henvender sig til personalet med spørgsmål til personoplysninger, gives henvendelsen omgående videre til leder.
Leder er ansvarlig for at besvare henvendelsen.

SAMTYKKE TIL BEHANDLING AF PERSONOPLYSNINGER

Vi har i visse tilfælde en pligt til at indhente GDPR-samtykke fra borgere, pårørende og andre.

GDPR-samtykke drejer sig kun om, at den pågældende siger ja eller nej til en specifik anvendelse af deres personoplysninger.

Samtykke med "ja" skal være givet i følgende tilfælde:

- Billeder/Video til offentliggørelse – fx på vores hjemmeside eller Nyhedsbreve eller lign.
- I forbindelse med at personale ansættes (i særlige tilfælde)

Oversigt over samtykker findes på kontoret.
Samtykke indhentes og administreres af daglig leder.

HÅNDTERING AF BILLEDER

Billeder og video med personer er personoplysninger.

Hvis der er den mindste mulighed for, at personer på billeder/video vil føle sig udstillet/krænket, må billedet og video ikke anvendes, og skal omgående slettes.

En forældre/medarbejder kan altid afvise, at der tages billeder af vedkommende eller barnet. Dette skal i så fald efterleves.

Billeder og video må behandles, når de kan henføres til vores arbejde.
Der må ikke tages flere billeder end nødvendigt.
Billeder må være på hjemmesider mv., så længe samtykke forefindes, og så længe forældre eller medarbejder er tilknyttet institutionen.

Trækkes et samtykke tilbage, skal offentliggjorte billeder slettes.
Alternativt skal personen sløres.
Hvis billeder findes i trykte medier, er der ikke krav om sletning, men må ikke genanvendes.

Billeder til historiske formål (begrænset) må gemmes så længe der er et formål hermed og dette kan begrundes.

Billeder på telefoner, tablets, billedarkiver i øvrigt skal slettes jf. sletteregler herunder.

HÅNDTERING AF PERSONDATABRUD

Persondatabrud skal håndteres med det samme, når det opdages.

Hvis en medarbejder bliver bekendt med, eller mistænker at, der er sket et persondatabrud, skal vedkommende ***med det samme*** kontakte ***daglig leder.***

BRUG AF COMPUTER, TABLETS, TELEFONER mv. (enheder)

Alle enheder skal låses, når de ikke anvendes / forlades. Skærmlås med kode og en pinkode skal være aktiveret med kort interval.

IPads og telefoner skal opbevares i aflåste kontor udenfor arbejdstid.

Enheder må ikke anvendes til opbevaring / midlertidig opbevaring af filer / dokumenter med personoplysninger – men skal overføres til Aula.

Billeder og video skal tages med institutionen telefoner / IPads.

USB-stik kan kun anvendes med godkendelse fra daglig leder.
Medarbejdere har et medansvar for oprydning på de forskellige enheder.
Enheder skal være under opsyn.
Bliver en enhed tabt eller stjålet, skal leder straks underrettes.

Der må ikke anvendes private enheder i arbejdssammenhæng.

BRUG AF SYSTEMER, TJENESTER OG MAIL

Alle medarbejdere får et personligt brugernavn og kodeord til vores systemer, når de bliver ansat. Kodeord er personligt, og må ikke deles med andre.
Alle medarbejdere er ansvarlige for at deres kodeord skiftes minimum hver ½ år.

Institutionens mail må som udgangspunkt kun anvendes til arbejdsrelaterede formål.