BESTIL PDF/UA

BESKYTTELSE AF PERSONOPLYSNINGER

for skolerne i Nyborg Kommune

Nyborg KOMMUNE

Beskyttelse af personlige data

Folkeskolen håndterer i en række sammenhænge oplysninger om de enkelte elever. Det er vigtigt, at håndteringen af sådanne oplysninger sker på en måde, der sikrer integritet og sikkerhed om personoplysningerne, så elever og forældre har tillid til skolen.

Samtidig skal folkeskolens håndtering af oplysningerne være gennemsigtig, så det står klart for elever og forældre, hvornår der behandles personoplysninger, og hvilke oplysninger der behandles.

Med den nye persondataforordning har der vist sig et behov for at få præciseret reglerne for opbevaring og behandling af persondata. Denne folder har til formål, særligt for skoleområdet, at beskrive:

- forskellen på følsomme/fortrolige persondata kontra almindelige persondata
- hvilke IT-løsninger skolerne har til rådighed, og hvornår de anvendes i forbindelse med kommunikation og opbevaring af persondata
- hvem må have adgang til hvilke data
- hvilke data må indhentes, og i hvilket omfang må de gemmes

Aula i 2019

Aula gik i luften i efteråret 2019 som erstatning for SkoleIntra.

Aula må i vid udstrækning bruges til håndtering af data i et omfang, som en række af de nuværende systemer ikke kan.

Hvad er følsomme og fortrolige personoplysninger?

Personoplysninger er oplysninger, der kan identificere en person. Der skelnes i lovgivningen mellem almindelige personoplysninger - der ikke er beskyttede - kontra oplysninger, der er fortrolige eller følsomme.

I Nyborg Kommuner skelner vi ikke mellem fortrolige og følsomme personoplysninger, da vi altid skal behandle og opbevare disse persondata varsomt og i sikre it-systemer – fremover benævnes disse data som 'følsomme'.

Tilsvarende skal vi, når vi kommunikerer med forældre, kollegaer og eksterne samarbejdspartnere være opmærksomme på vores tavshedspligt og anvende sikre kommunikationskanaler, når indholdet er følsomt.

Tåler dine persondata at blive udsendt på et åbent postkort?

I praksis opfatter vi følsomme persondata som data, der ikke tåler at blive sendt ud på et 'åbent postkort'. Listen er lang, men for skoleområdet kan nævnes oplysninger som:

- CPR-nummer
- Beskyttet adresse
- Familiestridigheder
- Tvangsfjernelse af børn
- Misbrug
- Helbredsoplysninger
- Arbejdsløshed
- Separation- og skilsmisse
- Seksuel orientering
- Portrætbilleder
- Økonomi, gæld, løn
- Strafbare forhold
- Væsentlige sociale problemer
- Kontaktoplysninger med foto, telefonnummer, mail- og privatadresser
- Fremmøde og fravær
- Evalueringer af de enkelte elevers faglige udbytte og personlige udvikling
- Karakterer og resultater i de nationale tests
- M.fl.

De generelle principper for behandling af data

- skal overholdes hver gang, der behandles personoplysninger.

Lovlighed

Formålet med behandlingen af data skal være lovlig.

Det vil sige baseret på databeskyttelsesforordningen, anden lov eller samtykke fra personen selv.

Rimelighed

Databehandlingen skal være rimelig og korrekt. Oplysningerne:

- Skal være tilstrækkelige, relevante og korrekte
- Skal være begrænset til, hvad der er nødvendigt i forhold til formålet
- Må ikke opbevares længere end nødvendigt - se også side 7

Gennemsigtighed

Den registrerede skal kunne gennemskue, hvad data bruges til.
Registrerede skal oplyses om:

- Rettigheder
- Formål med behandlingen af data
- Det legitime grundlag for behandlingen
- Tidspunktet for sletning af data

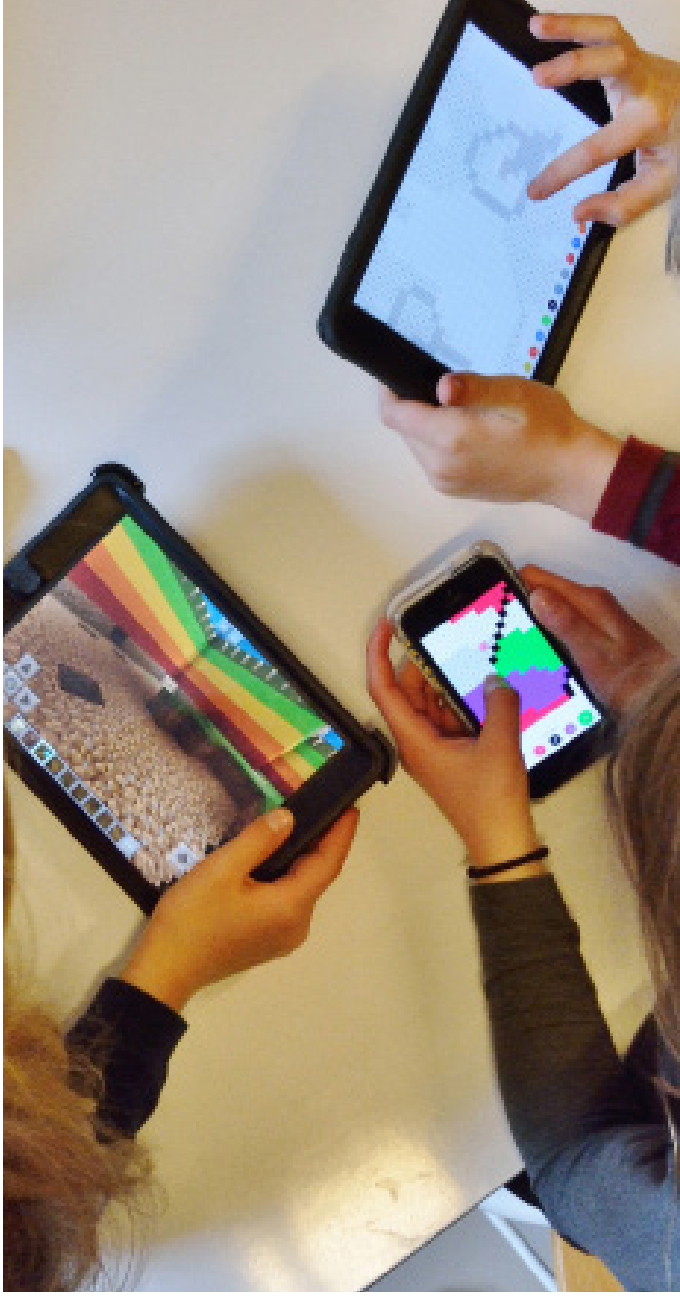
Syv hovedregler i databehandling

1. **Lovlighed, rimelighed og gennemsigtighed:** Borgerne ejer deres egne oplysninger, og det offentlige må kun have dem liggende og arbejde med dem, hvis der er et lovligt og rimeligt formål hermed, og hvis borgerne er informerede om, at det sker.
2. **Formålsbestemthed:** Behandling af data skal ske ud fra saglige og legitime formål. Hvis borgeren har givet tilladelse til databehandling ud fra ét formål, så gælder tilladelsen kun til dette formål.
3. **Dataminimering og proportionalitet:** Man må kun indsamle, gemme og arbejde med data som er tilstrækkelige, relevante og begrænsede til det, der er nødvendigt, dvs. ”need to know” og ikke ”nice to know”.
4. **Datakvalitet:** Personoplysninger skal være korrekte og ajourførte. Urigtige oplysninger skal slettes eller korrigeres. Personoplysninger skal derfor kunne opdateres eller slettes i alle it-systemer.
5. **Opbevaringsbegrænsning:** Personoplysninger skal slettes eller anonymiseres, når man ikke længere har behov for at behandle dem. Det skal derfor konkret afgøres i hvor lang tid forskellige typer af personoplysninger skal gemmes og må behandles.
   Der skal være en slettepolitik og sletteprocedure, der sikrer dette. Den enkelte skoleledelse har ansvaret herfor.
6. **Integritet og fortrolighed:** Data må kun opbevares og behandles i systemer, som giver den nødvendige sikkerhed.
7. **Sund fornuft:** Brug din sunde fornuft og tag rimelige forholdsregler. Vurdér risiko og sandsynlighed for, at der kan ske brud på databeskyttelsen.

Sikre og usikre systemer

Hovedreglen er, at de kommunale it-systemer er sikre – men på forskellig vis – mens private eller webbaserede systemer sjældent er det. Der skal foreligge en databehandleraftale på systemerne, og der skal være procedurer, der sikrer, at data f.eks. ikke opbevares længere end de må, og at kun de relevante personer har adgang til data. Ansvaret for dette påhviler den enkelte skoleledelse.

- Pædagogiske platforme som Aula og MeeBook opfylder de tekniske sikkerhedskrav, men der skal være procedurer for, hvem der må se og bruge hvilke oplysninger. Den lokale skoleledelse har ansvaret herfor.
- **FilR** kan anvendes til sikker opbevaring af alle slags dokumenter. Bemærk, at dokumenter gemt under ”Mine Filer” slettes ved ansættelsens ophør.
- Elevadministrationssystemet **Tabulex Tea** opfylder de tekniske sikkerhedskrav, men der skal være procedureregler for, hvem der må se og bruge hvilke oplysninger. Den lokale skoleledelse har ansvaret herfor.
- Kommunale mailsystemer opfylder som hovedregel sikkerhedskravene, mens web-baserede mailsystemer som hotmail, Gmail mv. ikke gør det. **Aula** og **”Send sikkert” i Outlook** er den sikreste måde at kommunikere digitalt med forældrene på. Mellem medarbejdere i Nyborg Kommune kan du kommunikere sikkert med din nyborg.dk-mail.
- Sociale medier som Facebook, Twitter, Snapchat, YouTube m.v. opfylder generelt ikke sikkerhedskravene og må derfor ikke anvendes til personoplysninger. Dette gælder både tekst og billeder med mindre der er indhentet konkret skriftlig tilladelse.
- Webbaserede fildelingssystemer som f.eks. Google Drev, Dropbox, iCloud mv. opfylder generelt ikke sikkerhedskravene, og må kun anvendes i overensstemmelse med Nyborg Kommunes interne retningslinjer for indkøb og brug af filopbevaringssytemer i cloudløsninger. Det betyder bl.a., at der ikke må opbevares fortrolige og følsomme personoplysninger i fildelingssystemerne.
- **KMD Sag/Nova** (ESDH-system) opfylder sikkerhedskravene, hvis de forskellige sikkerheds- og procedureregler bliver fulgt.



Sikker kommunikation i Nyborg Kommune

Skolerne i Nyborg Kommune har en række IT-løsninger til rådighed, hvorfra kommunikation til forskellige målgrupper finder sted. I nedenstående skitseres, hvilke IT-løsninger, der skal anvendes til sikker kommunikation - det vil sige kommunikation, der indeholder følsomme persondata.

	Sikker kommunikation?	Beskrivelse
Aula	Ja, til intern kommunikation med elever, forældre og kollegaer	Lukket IT-miljø, hvor brugerne logger på via Uni-login – mulighed for at ’steppe-up’ med ekstra kode for indhold, der betragtes som ’følsomt’
Outlook	Kun sikker ved kommunikation til kollegaer i Nyborg Kommune med @nyborg.dk som mail-efternavn.	Almindeligt mailsystem, der ved udsendelse af mails uden for firewall er ”hackbart” og svarer til et åbent postkort.
Outlooks ’Send Sikkert-knappen’	Sikker mail	Udfyld modtagerens CPR, CVR eller sikkermailadresse i adressefeltet og tryk ’Send Sikkert’ (modtages i eBoks ved anvendelse af CPR/CVR).

Sikker opbevaring af data i Nyborg Kommune

I nedenstående er oplistet de IT-løsninger, hvori skolerne har adgang til opbevaring af data. Herudover vil en række administrative medarbejdere på skolerne skulle forholde sig til, hvornår dokumenter, breve og øvrige data skal journaliseres og/eller arkiveres.

HVILKE SIKKERHEDSKRAV OPFYLDER SYSTEMET?					
	Opfylder de generelle sikkerhedskrav	Må anvendes til opbevaring af personoplysning	Må anvendes til opbevaring af følsomme personoplysning	Kan/må anvendes til journalisering?*)	Udtræk til Statens Arkiver?
Aula (pr. august 2019)	Ja	Ja	Ja	Nej	Ja
FilR	Ja	Ja	Ja	Nej	Nej
MeeBook	Ja	Ja	Nej**)	Nej	Nej
KMD Sag/Nova	Ja	Ja	Ja	Ja	Ja
Tabulex Tea	Ja	Ja	Ja	Nej	Ja
Stafetlog	Ja	Ja	Ja	Nej	Nej
Outlook (nyborg.dk mail)	Nej (kun ved ”Send Sikkert” og interne mails)	Ja	Kun 30 dage	Nej	Nej
Øvrige (OneDrive, Google Drive, Dropbox mv.)	Nej	Ja***	Nej	Nej	Nej
Gmail, yahoomail, hotmail mv.	Nej	Nej	Nej	Nej	Nej

*) Ved journalisering forstås sikker opbevaring af (dokumenter, brev m.m.) som led i en ’administrativ sagsbehandling’, og som muliggør behandling af klagesager og anmodning om aktindsigt.

**) Dog kan karakterer, standpunktskarakterer og standpunktsudtalelser uden indehold af helbredsoplysninger tillades.

***) Anvendelse af øvrige systemer som f.eks. OneDrive kræver forudgående godkendelse i overensstemmelse med Nyborg Kommunes interne retningslinjer for indkøb og brug af filopbevaringssytemer i cloudløsninger.

Centrale anbefalinger om opbevaring og videregivelse af persondata

1. **Gem ikke persondata** på egen pc, på kommunale serverdrev eller i mail, men kun i sikre systemer. Gem dem aldrig på eksterne serverdrev, usb-nøgler m.v.
2. **Slet gamle mails.** Der må ikke ligge mails med følsomme persondata i mailsystemet længere end én måned. Gamle mails skal arkiveres sikkert, hvis de skal bevares.
3. **Send kun følsomme personoplysninger** via Aula, e-Boks eller Send Sikkert i Outlook (f.eks. afgørelser om specialundervisning, underretninger, testresultater og helbredsoplysninger).
4. **Slet gamle oplysninger** om tidligere elever i FilR minimum én gang om året. Offentliggør kun personoplysninger (tekst og billede) efter konkret tilladelse fra forældre.
5. **Skriv ikke personfølsomme oplysninger i overskriften** for kalenderaftaler og heller ikke i selve kalenderaftalen. Kalendere er åbne for alle.

Offentliggørelse af billeder

Datatilsynet ændrede praksis i september 2019. Spørgsmålet, om der vil kunne offentliggøres et billede på internettet uden samtykke fra den berørte person, beror nu på en helhedsvurdering af billedet og formålet med offentliggørelsen. Der vil være mulighed for at offentliggøre nogle portrætbilleder uden samtykke. Det skal konkret vurderes, om kommunen har grundlag for at offentliggøre billedet, samt om personen på billedet ikke med rimelighed kan føle sig udstillet, udnyttet eller krænket.

Orientering

Hvorvidt, om der skal ske orientering inden offentliggørelse af billeder afhænger af formålet. Er formålet at vise personen, skal der ske orientering, omvendt hvis formålet er at vise situationen fx et billede af en flok børn på tur med børnehaven eller skolen, vil der ikke skulle ske orientering inden offentliggørelse.

Hvis disse behandlingsgrundlag ikke er til stede, skal behandlingsgrundlaget være samtykke. Selvom der ikke er krav om indhentelse af samtykke, skal personen på billedet som udgangspunkt orienteres om, at man vil offentliggøre billedet, så personen har mulighed for at gøre indsigelse.

Når institutionen tager et billede/optager en video af et barn, er der tale om behandling af personoplysninger. Det kræver ikke samtykke fra forældrene, da der er tale om almindelig myndighedsudøvelse. Men nogle forældre bryder sig ikke om, at deres børn figurerer på billeder. Det er derfor en god idé at bede forældrene om at tage stilling til spørgsmålet om billeder/video, når barnet starter i institutionen. Et ønske fra forældrene om, at der ikke skal tages billeder af barnet, skal respekteres, og det er derfor vigtigt, at personalet får spurgt forældrene, hvordan de forholder sig til brug af billeder af deres børn.

Samtykke

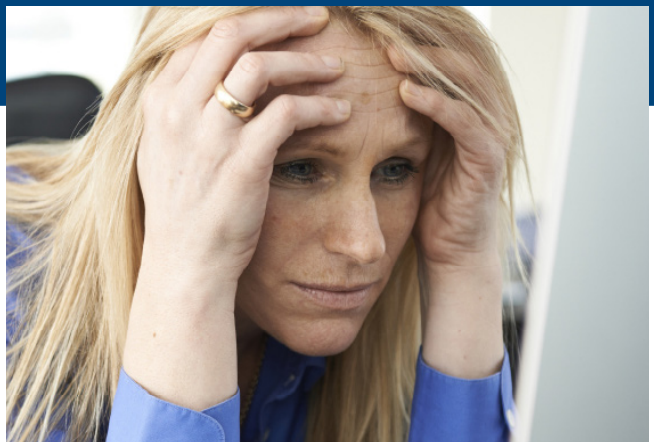
Der skal indhentes samtykke til offentliggørelse af billeder, såfremt personerne på billedet med rimelighed kan føle sig udstillet, udnyttet eller krænket. Samtykke skal kunne dokumenteres og der må ikke være tvivl om, hvilke billeder, der er givet samtykke til. Et samtykke kan altid trækkes tilbage, hvilket indebærer, at billedet ikke må benyttes fremadrettet. Hvis billedet f.eks. er trykt i en pjece, skal pjecen ikke trækkes tilbage, men der må ikke laves nye pjecer med billedet.

Når noget går galt:

Ved sikkerhedsbrud

Kontakt Digitalisering og I-sikkerhed på mail: dpo@nyborg.dk

Læs mere om databeskyttelse på hjemmesiden: www.nyborg.dk/da/OmKommunen/Databeskyttelse

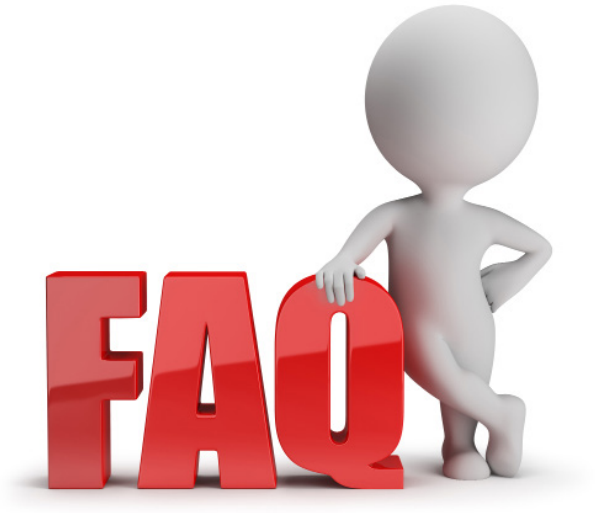


Spørgsmål

På side 7-9 kan du finde ofte stillede spørgsmål.

Har du yderligere spørgsmål til beskyttelse af personoplysninger i skolerne, kan du kontakte Digitalisering og I-sikkerhed på mail: digitalisering-og-i-sikkerhed@nyborg.dk

Ofte stillede spørgsmål



Hvor mange på skolen må inddrages i behandlingen af den enkelte elevs personoplysninger?

Folkeskolens behandling af elevers personoplysninger må kun ske til udtrykkeligt angivne og saglige formål, og behandlingen skal være relevant og begrænset til, hvad der er nødvendigt for formålet med opgaveløsningen.

Det er derfor ikke tilladt at afsøge, orientere sig i, tjekke op på eller videregive personoplysninger om de enkelte elever, hvis det ikke er nødvendigt for den konkrete opgavevaretagelse omkring eleven. Det gælder også, selv om man rent teknisk måtte have adgang til oplysningerne.

Adgangen til at udveksle personoplysninger om den enkelte elev afhænger derfor af, om de enkelte medarbejdere har brug for oplysninger om eleven til varetagelse af medarbejderens arbejdsopgave i regi af skolen. Det kan f.eks. være berettiget, at de lærere, som underviser samme klasse, får adgang til oplysninger på individniveau om eleven (f.eks. testresultater), navnlig hvis lærerne arbejder sammen i team, ligesom læreren kan drøfte spørgsmål om de enkelte elever med skolens pædagogiske leder.

Har forældre ret til at vide, hvilke oplysninger skolen behandler om barnet?

Forældremyndighedens indehaver har som udgangspunkt ret til at få oplyst, hvilke oplysninger skolen har registreret om barnet. Det kaldes ”indsigtsret”.

Forældremyndighedsindehaveren har ret til at få at vide, hvilke oplysninger, der behandles om barnet, formålet med behandlingen, hvor oplysningerne kommer fra og hvor længe de vil blive behandlet.

Forældremyndighedsindehaverens ret til indsigt kan begrænses, hvis dennes interesse i at få kendskab til oplysningerne ”bør vige for afgørende hensyn til offentlige eller private interesser”, herunder hensynet til barnet selv. Hvis skolen ikke vil give indsigt i skolens oplysninger om barnet, kan forældrene klage til Datatilsynet.

Hvor længe må følsomme personoplysninger om et barn/en elev ligge i de forskellige systemer, og hvem har ansvaret for at slette dem?

Persondata må være registreret i de forskellige systemer, så længe det er fagligt relevant og i overensstemmelse med formålet med registreringen. Typisk slettes data senest 10 år efter, at barnets undervisningspligt er opfyldt.

Bemærk, at eksamensbeviser og nødvendige data for at udstede sådanne beviser skal gemmes.

Elevsager, herunder elevplaner m.v., skal ikke gemmes, med mindre det vurderes relevant. Der skal altså foretages en konkret vurdering.

Kræver det konkret samtykke (tilladelse) fra forældrene, hvis man registrerer oplysninger om et barns sociale, personlige eller læringsmæssige udvikling (herunder specialundervisning) på egen pc eller i skolens digitale læringsplatform? Skal forældrene informeres om registrering?

Det kræver ikke tilladelse fra forældrene at registrere oplysninger, hvis det sker som del af den opgave, som man skal løse. Men forældrene skal som hovedregel informeres om, hvilke oplysninger der registreres. Sådanne oplysninger må alene blive gemt i sikre systemer og således ikke på ens egen pc. Data skal slettes igen, når de ikke længere er relevante at opbevare.

Må man have en klasse-/gruppeliste med navne, adresser, telefonnumre og mailoplysninger på skolens internetside, i læringsplatformen eller i Aula – eller kræver det årligt samtykke fra forældrene?

En klasseliste indeholder persondata. Det kræver derfor samtykke fra forældrene at offentliggøre sådanne. Det anbefales at sådanne oplysninger ikke placeres på en offentlig tilgængelig hjemmeside, men kun i lukkede systemer (f.eks. intranet eller Aula) og at der indhentes samtykke.

Må en skole føre en løbende oversigt over, hvilke støttetiltag der er igangsat for de forskellige elever (f.eks. specialundervisning, støtte til fysiske handicap, igangsatte underretninger)?

Ja, så længe det sker i et sikkert system, så længe data er ajourførte, og så længe forældrene er informeret om de data, der registreres.

Hvis man får en mail fra en forældres hotmail-adresse vedr. deres barns specialundervisningsbehov, må man så svare, eller skal man svare via Aula eller til e-Boks?

Svar skal sendes via sikker mail dvs. via Aula eller ”Send sikkert” i Outlook.

Hvad er reglerne for opbevaring og sletning af data eller billeder af børn/elever på mobiltelefon og iPad?

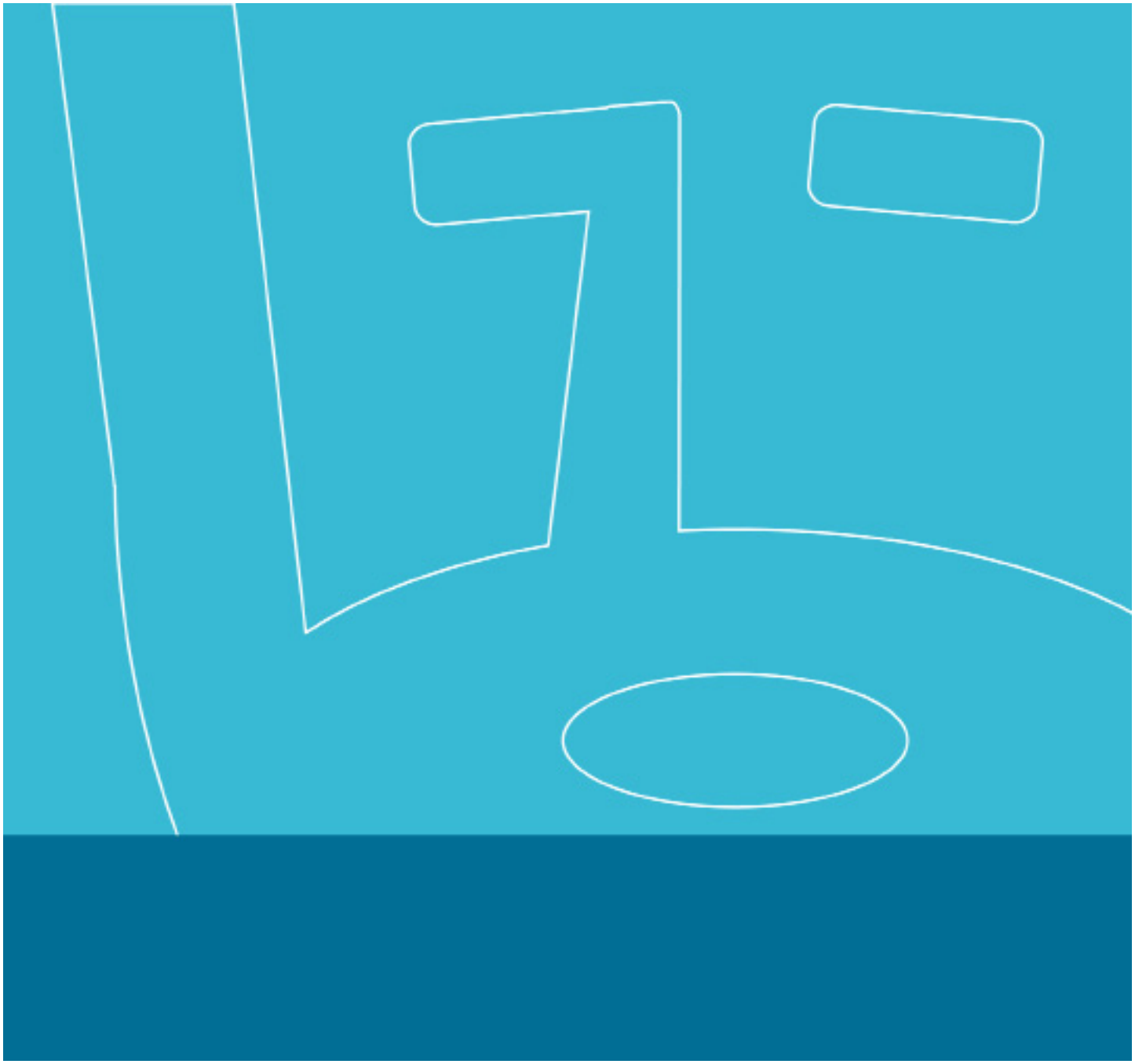
Opbevaring og anvendelse af portrætbilleder kræver skriftligt samtykke fra forældrene. Billeder skal altid gemmes i et sikkert system, som hovedregel i Aula eller FilR. Portrætbilleder skal hurtigst muligt overføres til et sikkert system - hvor samtykke også registreres - og bør slettes straks efter på den mobile enhed. Skoleledelsen sikrer procedurer for sletning af billeder på mobile enheder.

Er lærere og pædagoger omfattet af forvaltningslovens bestemmelser om journal- og notatpligt?

Forvaltningsloven omfatter alle offentlige myndigheder, også skoler og institutioner. Men den sigter mod forvaltningsvirksomhed, hvor der er eller vil blive truffet en afgørelse. Faktisk forvaltningsvirksomhed som f.eks. undervisning, pædagogiske aktiviteter, pasning mv. er ikke omfattet af forvaltningsloven. Det betyder f.eks., at en lærer eller en pædagog ikke er omfattet af reglerne om f.eks. notatpligt, journalisering m.v. så længe det handler om den almindelige praksis. Men når der træffes beslutning, hvor der udøves myndighed, gælder lovens bestemmelser. F.eks. når der træffes beslutning om underretning, igangsættelse af specialpædagogiske tiltag, disciplinære foranstaltninger og henvendelser vedr. mobning m.v.

Hvordan må personoplysninger om medarbejdere behandles? – Må en oversigt over hvem, der er fraværende pga. sygdom eller barns sygdom f.eks. hænge i personalerummet, så alle kan se det?

Personoplysninger om sygdom må ikke være offentligt tilgængelige. Men det må gerne fremgå, hvem der er tilstede, og hvem der ikke er, så længe årsagen ikke fremgår.



Opdateret december 2020

Nyborg
KOMMUNE

Torvet 1
5800 Nyborg
www.nyborg.dk