Instruks til ansatte ved Børnenes Friskole om behandling af personoplysninger

Opbevaring af og adgang til personoplysninger:

Ansatte har pligt til altid at opbevare dokumenter eller udstyr med personoplysninger forsvarligt og utilgængeligt for uvedkommende.

Det betyder blandt andet at:

- Computer, telefoner og lignende udstyr, der bruges til arbejdsrelaterede mails mv., ikke efterlades uden låst skærm.

- Computer og lignende udstyr (f.eks. USB-stik, telefoner, harddiske eller tablets) skal opbevares på sikker vis og ikke må efterlades på offentlige steder eller på uovervågede/uaflåste steder på arbejdspladsen.

- Dokumenter (elektroniske såvel som på papir!!) der indeholder personoplysninger skal altid opbevares på en måde, hvor kun relevante personer har adgang.

- Særligt følsomme dokumenter må ikke ligge i taske eller lignende, men skal opbevares i arkiv eller aflåste personaleskabe.

- Elektroniske dokumenter og data indeholdende personoplysninger skal opbevares på udstyr udleveret af skolen – eksempelvis computer, ekstern harddisk, USB, skolens server eller cloud-baserede systemer.

- Fysiske dokumenter og notater skal opbevares forsvarligt og i videst mulige omfang kun på skolen.

- Computer og lignende udstyr er sikret med kode – se mere om sikkerhed nedenfor.

- Post indeholdende personoplysninger lægges i barnets mappe i arkivet. Kontoret sender en mail til modtager af brevet.

Brug af mail og internet

Alt kommunikation vedr. arbejde, mellem ansatte , elever og forældre, skal foregå via mailadresserne som er tilknyttet G-mailsystemet boernenesfriskole.dk eller SkoleKom-konferrencen på Børnenes Friskole. Det er ikke tilladt at bruge sin private mail til arbejdsrelateret korrespondance. Fortrolige/følsomme personoplysninger som sendes "ud af huset" skal altid sendes via en sikker mail løsning – eBoks fra kontoret. Proceduren er, at man gemmer på en USB-nøgle, mailer til kontoret@boernenesfriskole.dk, eller via indscanning fra kopimaskinen til kontoret@boernenesfriskole.dk og får kontorpersonalet til at sende til rette modtager.

Hvis der modtages personoplysninger (f.eks. vedr. helbredsoplysninger etc.), som er tilsendt med ikke sikker mail, skal disse hurtigst muligt overføres til en sikker opbevaringsmetode og mailen slettes.

Google-Education har vi på BØF klassificeret som intern sikker mail/intern sikkert område. Man skal være YDERST opmærksom på ikke at dele mapper og dokumenter med andre (herunder børn og forældre), end de kollegaer man ønsker at dele med.
E-boks er klassificeret som sikker mail ("ud af huset").

Brug af privat mobiltelefon

Det er ikke tilladt at bruge privat mobiltelefon til sende beskeder indeholdende personoplysninger eller til at tage billeder eller optage videoer af elever og forældre.

Såfremt der skal tages billeder eller video af elever og forældre benyttes skolens kameraer eller en af skolens mobiltelefoner (ledelsens eller kontorets mobiltelefoner).

Såfremt man har adgang til mail og Google-drev via sin private mobiltelefon, skal reglerne for sikkerhed være aktiveret (se nedenfor).

Brug af sociale medier

Personoplysninger må aldrig deles på sociale medier. Såfremt der skal deles billeder, videoer eller lignende skal det foregå på skolens officielle profiler og sider, og kun hvis der er givet samtykke fra forældrene - (Man skal således orientere sig på kontoret om der er nogle af børnene/forældrene, som ikke har givet samtykke til dette).

Samtaler i det offentlige rum

Det er ikke tilladt at føre samtaler i det offentlige rum, som gør det muligt for omkringværende børn og voksne at identificere de elever eller forældre det drejer sig om.

Adgang til elevmapper

Efter aftale med kontoret/ledelsen kan man som ansat få adgang til relevante elevmapper.

Sikkerhed

IT-udstyr og papirer der indeholder eller giver adgang til følsomme oplysninger – herunder navnlig personfølsomme oplysninger skal altid håndteres under iagttagelse af passende sikkerhed. Det betyder for eksempel:

- At koder skal indeholde mindst 8 tegn
- At kodeord/passwords ikke genbruges til flere tjenester
- At koder skiftes med passende mellemrum – fx hver tredje måned
- At koder/passwords opbevares sikkert og adskilt fra udstyret – undgå, om muligt, at nedskrive kodeord/password
- At man skal låse sin skærm når man går fra computer/mobiltelefon
- At man ikke åbner mistænkelige mails og hjemmesider
- At mails indeholdende data med personfølsomme oplysninger, ikke videresendes, medmindre det er strengt nødvendigt, f.eks. i forbindelse med myndighedsbehandling – og at det i givet fald sker via sikker mail.

Sikkerhedsbrud

Ansatte har pligt til, hurtigst muligt, at give skolens ledelse meddelelse om formodede eller konstaterede sikkerhedsbrud.