***Inspiration til skolens instruks til ansatte***

*Skolens ledelse skal sikre sig, at alle ansatte har modtaget informationen (/instruks) om, hvordan data/oplysninger der indeholder personoplysninger skal håndteres og opbevares. Information bør også omfatte mere generelle regler om brug af it, mail, intranet m.v.*

*Formålet med denne inspirations-tekst er at give skolen et udgangspunkt for at udfærdige en information/instruks til medarbejderne, som er tilpasset forholdene på netop jeres skole.*

*Bemærk, at det kan være aktuelt, at andre end skolens medarbejdere modtager en instruks – fx bestyrelsens medlemmer eller andre med adgang til dokumenter med følsomt indhold herunder personoplysninger.*

*Friskolernes Hus foreslår, at den færdige instruks indsættes i skolens Persondatamappe.*

 **Skabelon:**

 **Instruks til ansatte ved [SKOLE] 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 og lignende udstyr ikke efterlades uden låst skærm.
* Computer og lignende udstyr (fx 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.
* 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.

**Brug af mail og intranet**

Det er ikke tilladt at bruge sin private mail til arbejdsrelateret korrespondance. Personoplysninger skal altid sendes via en sikker mail løsning eller via skolens intranet [navn]. Skriftlig kommunikation skal desuden altid leve op til skolens politik/instruks på området.

Hvis der modtages personoplysninger, som er tilsendt med ikke sikker mail, skal disse hurtigst muligt overføres til en sikker opbevaringsmetode og mailen slettes.

**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 [hvad?].

**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. [Procedure for hvordan det skal gøres].

**Samtaler i det offentlige rum**

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

**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 ikke åbner mistænkelige mails og hjemmesider
* At mails indeholdende data med personfølsomme oplysninger, som ikke videresendes, medmindre det er strengt nødvendigt, fx 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.

**Skolens IT-politiker**

Alle ansatte har pligt til at gøre sig bekendt med skolens IT-politikker.