***Læse- og brugsvejledning til Instruks til ansatte om behandling af personoplysninger:***

*Skolens ledelse har pligt til at 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.*

*Den færdige instruks kan med fordel indsættes i skolens Persondatamappe.*

**Instruks til ansatte på [EFTERSKOLE] om behandling af personoplysninger**

Denne instruks beskriver de regler og retningslinjer, der gælder for medarbejdernes omgang med og behandling af personoplysninger om elever og forældre på [EFTERSKOLE].

**Tavshedspligt og persondata**

Alle ansatte på efterskoler er omfattet af forvaltningslovens regler om tavshedspligt. Det betyder, at oplysninger om elever og forældre, som kommer til ens kendskab i kraft af arbejdet på skolen, ikke må deles med udenforstående. Det er derfor fx ikke tilladt at føre samtaler i det offentlige rum, som gør det muligt for omkringværende at identificere de elever eller forældre samtalen drejer sig om.

**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 ikke må efterlades på offentlige steder
* Dokumenter skal 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 cloudbaserede systemer
* Fysiske dokumenter og notater skal opbevares forsvarligt og i videst mulige omfang kun på skolen
* Computer og lignende udstyr er sikret med kode.
* Krav til kode er, at du skifter mindst X gange årligt. Du må ikke bruge samme kode til din arbejdskonto/mail, som du bruger privat.

**Brug af mail og intranet**

Det er ikke tilladt at bruge sin private mail til arbejdsrelateret korrespondance.

Personoplysninger skal altid sendes via [skolens 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. Du må ikke svare på mailen via en usikker forbindelse.

**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 [kamera/arbejdstelefon].

**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. [Indsæt procedure for, hvordan det skal gøres, jf. regler om samtykke til brug af billeder].

**Sikkerhedsbrud**

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

**Skolens IT-politikker**

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