bilag 11 – tekniske og organisatoriske   
sikkerhedsforanstaltninger

**ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER:**

|  |  |  |
| --- | --- | --- |
| **EMNE** | **RETNINGSLINJER** | **KONKRETE PROCEDURER** |
| **Fysiske personers adgang til IT-systemer:** | **Adgangsbegrænsning:**  Det sikres, at kun de medarbejdere, det er relevant for, har adgang til de IT-systemer, hvori der opbevares personoplysninger. | Der etableres et autorisationssystem, hvor hver enkelt medarbejder får et individuelt og unikt brugernavn til individuel brugerprofil (brugernavne genbruges aldrig, selvom medarbejderen er fratrådt).  Når en medarbejder fratræder, slettes brugerprofilen straks. |
| **Adgangskoder:**  Det sikres, at kun den enkelte medarbejder, kan få adgang til medarbejderens ”brugerprofil” på IT-systemet. | Alle medarbejdere har en egen og individuel adgangskode.  Medarbejderens pc er opsat til at logge ind med uni-login.  Der må ikke anvendes standardkoder.  Alle arbejdsstationer låser efter 45 minutters inaktivitet, og låses op igen med individuel skærmlås.  Hvis man forlader sin pc, skal den låses med + L eller lukke skærmen ned.  Der kan ønskes kortere tid før pc låses.  I det omfang, det er muligt i de brugte IT-systemer, anvendes 2-faktorkoder.  Det er forbudt at give tilladelse til, at brugernavn og adgangskode huskes – dette gælder for både hardware og software. |
| **E-mails:** | **Brug af sikker/krypteret mail:**  Der bruges altid sikker/krypteret mail ved fremsendelse af e-mails indeholdende personoplysninger om CPR-numre, strafbare forhold og særligt følsomme personoplysninger. | LN, GFK, HH, HJ, har alle mulighed for at sende sikre mail via e-boks.  Alle sikre mails, der skal sendes ud af huset sendes fra disse mailkonti. |
| **Arkivering af e-mails:**  Alle mails, der indeholder personoplysninger, og som er relevante at gemme arkiveres uden for indbakken. | Relevante mails gemmes i barnets/elevens/medarbejderens mappe på Clouden eller på Skoleintra. |
| **Oprydning i indbakke, sendt post og slettet post:**  Der rydes jævnligt op i indbakke, sendt post og slettet post, så der ikke gemmes mails med personoplysninger i disse mapper. | Minimum én gang om ugen ryddes der op i indbakke, sendt post og slettet post. |
| **Data på mobile enheder:** | **Opbevaring af data på enheder stillet til rådighed af organisationen:**  Der må alene opbevares personoplysninger på mobile enheder (telefoner, ipads, laptops, USB-stiks m.v.), såfremt disse enheder er beskyttet med et sikkerhedsgodkendt krypteringsprogram. |  |
| **Opbevaring af data på private enheder:**  Der må ikke opbevares eller flyttes personoplysninger på private enheder. |  |
| **Papir:** | **Papirudskrifter:**  Det efterstræbes at al behandling af personoplysninger i organisationen foregår digitalt, og at udskrift eller anden form for håndtering af personoplysninger i papirform begrænses i videst muligt omfang. | Intet i papirform, der indeholder personoplysninger, forlader matriklen.  Alt papir med personfølsommeoplysninger makuleres straks efter brug. |
| **Uddannelse og introduktion:** | **Eksisterende medarbejdere:**  Alle medarbejdere, der er ansat i organisationen på tidspunktet for Datapolitikkens udarbejdelse, og som behandler personoplysninger, undervises i alle relevante dele af Datapolitikken. | Alle medarbejdere undervises minimum én gang hvert år i udvalgte og relevante emner fra datapolitikken. |
|  | **Nye medarbejdere:**  Alle nye medarbejder introduceres for Datapolitikken og forpligtelserne heri så hurtigt som muligt efter ansættelsesforholdets tiltrædelse. |  |
| **Kontrol:** | **Stikprøvekontrol:**  Der føres løbende stikprøvekontrol med, at alle de organisatoriske sikkerhedsforanstaltninger overholdes i hele organisationen. | Der føres stikprøvekontrol én gang i kvartalet med, at alle procedurer overholdes.  Stikprøvekontrollerne dokumenteres i årshjulet (bilag 1). |

**TEKNISKE SIKKERHEDSFORANSTALTNINGER:**

|  |  |  |
| --- | --- | --- |
| **EMNE** | **RETNINGSLINJER** | **KONKRETE PROCEDURER** |
| **Teknisk beskyttelse mod uautoriseret adgang:** | **Beskyttelse mod vira:**  Alle IT-systemer og –enheder beskyttes mod uautoriseret adgang ved opsætning af de nødvendige sikkerhedsforanstaltninger. | Alle pc’er opsættes med adgangskode. Beskyttes med firewall og Windows sikkerhed. |
| **Netværkssikkerhed:**  Alle netværk i organisationen er opsat med de nødvendige sikkerhedsforanstaltninger med henblik på beskyttelse mod autoriseret brug og adgang. |  |
| **Sikkerhedskopiering:** | **Back up:**  Alle systemer i organisationen, hvor der opbevares personoplysninger, sikkerhedskopieres jævnligt, så al data kan gendannes i tilfælde af fejl. | Der er ikke dataserverer på skolen. Alt foregår via portaler.  Easyiq/TEAMS kan gendannes indenfor 30 dage. |
| **Kryptering af data:** | **Brug af sikker/krypteret mail:**  Der bruges altid sikker/krypteret mail ved fremsendelse af e-mails indeholdende personoplysninger om CPR-numre, strafbare forhold og særligt følsomme personoplysninger. | Alle personfølsom oplysninger sender via e-boks. Ellers låses filen med koden, som sendes til modtagers mobiltelefon. |