Greve Gymnasiums leveregler for datasikkerhed

Nedenstående er nogle bud på, hvordan vi udøver persondatabeskyttelse og informationssikkerhed på i det daglige. Listen er ikke udtømmende:

1. Brug **passwords** (eller fingeraftryk som adgangskode) på din computer, ipad og smartphone og opdater med et nyt, unikt password hver gang systemet beder om det (hvilket på computeren er hver 6. måned) – eller oftere. Husk dit password og undlad at skrive det ned. Et password må under ingen omstændigheder fremgå af fx note it's, der sidder på din computeren. Tast aldrig dit password mens din computer er koblet til en storskærm eller lignende, hvor passwordet kan aflures

2. Aktivér din pauseskærm, hver gang du forlader din computer/iPad

3. Din arbejdscomputer/iPad må kun benyttes af dig. Den må ikke lånes ud til andre.

4. Udvis **fortrolighed** om de personoplysninger, du bliver bekendt med som led i dine arbejdsopgaver – del og videregiv ikke personoplysninger uden at være sikker på, at det er i orden

5. Efterlad ikke **fysiske dokumenter** med personoplysninger f.eks. karakterer fremme.

6. Papirdokumenter med personoplysninger skal altid bortskaffes ved **makulering**

7. **Print** der indeholder personoplysninger hentes i printeren straks. Overvej hvad du printer.

8. **E-mails** med fortrolige og følsomme personoplysninger sendes via E-Boks eller Sikker Mail til modtagere udenfor Greve Gymnasium.

9. Hvis personoplysningerne er modtaget eller sendt via **e-mail**, slettes mailen i Outlook senest 1 måned efter sagsbehandlingen er afsluttet. Mail med **følsomme** personoplysninger slettes efter en uge.

10. Overvej altid om det er nødvendigt at sende følsomme personoplysninger via mail.

11. Lav en rutine, hvor du sletter gamle mails og dokumenter, der indeholder personoplysninger. Tøm papirkurven på skrivebordet og tøm mappen slette mails.

12. Undlad altid at gemme personoplysninger på USB-nøgle, på skrivebordet på din bærbare computer eller lignende **usikre steder**.

13. Tag ikke nye it-systemer eller digitale platforme i brug uden at der først er sket en vurdering af sikkerheden i systemet. Det skal være frivilligt for eleverne om de vil afgive oplysninger til apps f.eks. Endomondo.

14. Åben ikke mails der ser mistænkelige ud eller som kommer fra afsendere, du ikke kender

15. Kontakt IT-administrator, hvis du bliver opmærksom på noget mistænkeligt