April 2018

Brøndby Gymnasiums regler om sikker databehandling

Når man som medarbejder på Brøndby Gymnasium behandler fortrolige eller følsomme personoplysninger om elever og medarbejdere, skal oplysningerne opbevares i de administrative systemer, som Brøndby Gymnasium har godkendt, hvilket er følgende systemer:

- DocuNote ESDH
- Bluegarden – Dataløn
- C5
- MobilePay
- Place2Book

Disse systemer er sikre, fordi der tages back up, benyttes firewall og antivirus, anvendes log-in, sker systemlogning af al aktivitet i systemet og fordi systemerne kun kan tilgås af de medarbejdere, der har arbejdsmæssigt behov for det.

Der må ikke gemmes fortrolige eller følsomme personoplysninger i andre systemer eller på andre platforme, fx eget drev, skrivebordet på computeren, Outlook, Lectio, Hotmail, Meebook, EduLife, GoogleApps, Skydrive, Dropbox, USB-sticks, mv. da disse af flere årsager ikke er sikre. [1]

Brøndby Gymnasium er dog opmærksom på, at mange dokumenter med personoplysninger i praksis "fødes", modtages eller midlertidigt opbevares i et it-system, der ikke fremgår af ovenstående liste over godkendte it-systemer, fx Outlook eller Lectio.

Når dette er tilfældet (og hvis dokumentet indeholder fortrolige eller følsomme personoplysninger[2]) skal det overføres til et af de godkendte it-systemer hurtigst muligt – dog senest 1 måned efter sagsbehandlingen er afsluttet.[3]

Samtidig med overførslen til et godkendt system slettes dokumentet effektivt fra det ikke-godkendte it-system, hvor det hidtil har været behandlet (fx mailboks, eget drev, skrivebordet, USB-stick, hjemme-pc, mv.)

Vedrørende Outlook skal man være opmærksom på, at kalenderaftaler kan være åbne for alle, og at der derfor ikke bør sendes kalenderindkaldelser med personoplysninger, der er fortrolige eller følsomme. Der bør i stedet henvises til den relevante sag i DokuNote ESDH.

[1] Årsagerne til at systemerne ikke er sikre er bl.a., at de mangler den lovkrævede logningsfunktion at BG ikke kender placeringen af og sikkerheden omkring den server, som oplysningerne befinder sig på samt at BG evt. ikke kan tilgå oplysningerne i tilfælde af en administrativ medarbejders længerevarende fravær, da BG ikke har administratoradgang til systemet.
[2] Hvis dokumentet ikke indeholder fortrolige eller følsomme personoplysninger er det ikke lovgivningsmæssigt krav om, at det overføres til et system, hvori der sker systemlogning. **Dog er der andre praktiske forhold, der taler for at dokumentet bør overføres til et af de godkendte systemer, herunder at der sker automatiseret sletning af oplysninger i fx DocuNote ESDH efter et forud defineret åremål**.
[3] Hvis et færdigt dokument skal opbevares i mindre end 1 måned (hvorefter det enten slettes eller anonymiseres), er der ikke lovgivningsmæssigt krav om, at det overføres til ESDH.

Brug af administrative systemer. Brugeradgange og rettigheder

Medarbejderne på Brøndby Gymnasium må kun behandle (dvs. bl.a. gemme) personoplysninger i de administrative it-systemer, som Brøndby Gymnasium har godkendt til formålet, jf. Retningslinjer Godkendte ITsystemer.

Den enkelte medarbejder på Brøndby Gymnasium gives autorisationer og rettigheder til it-systemerne ud fra en konkret vurdering af medarbejderens arbejdsopgaver.

Personlige adgangskoder til systemer med personoplysninger må ikke deles med andre medarbejdere og må kun "huskes" af systemet, hvis der er tale om en personlig computer.

Overflødiggjorte autorisationer lukkes.

Har man som medarbejder en autorisation, som (ikke længere) svarer til, hvad man har behov for til udførelse af sine arbejdsopgaver, men som derimod giver adgang til flere personoplysninger eller flere it-systemer, end hvad der er nødvendigt, skal man straks give ledelsen besked herom.

Det vil sige, at man som medarbejder selv skal reagere og kontakte sin nærmeste leder, hvis man har adgang til "for meget" eller "for lidt" – eller hvis man er i tvivl, om dette er tilfældet.

Det kontrolleres også løbende og mindst 2 gange årligt fra ledelsens side, at autorisationerne svarer til det saglige behov.

Fysisk sikkerhed for persondata

Vi skal forebygge, at uvedkommende får adgang til personoplysninger på Brøndby Gymnasium. Det gælder i særlig grad CPR-numre og andre fortrolige eller følsomme personoplysninger.

Derfor har vi følgende gode vaner:

- Fysiske dokumenter med **ind- og uddatamateriale**, der indeholder CPR-numre (og andre fortrolige eller følsomme personoplysninger) opbevares aflåst (i skuffe, skab eller kontor), når dokumentet ikke benyttes, og det makuleres efter endt brug.

- **Print** hentes i printeren straks. Sidste mand tjekker printer og makulator for glemte dokumenter, før kontoret forlades efter endt arbejdsdag.

- Alle medarbejdere på Brøndby Gymnasium sætter **låseskærm** på egen computer, når skrivebordet forlades i mere end få minutter. Låseskærm fremkommer ved kommandoen "*ALT + CTRL + DEL*". Ser man en medarbejders forladte skrivebord, hvor der ikke er sat låseskærm på computeren, gør man det for vedkommende.

- Ved **tyveri af udstyr** (fx computer, tablet og/eller smartphone, som man har fået udleveret som arbejdsredskab af Brøndby Gymnasium), skal man straks kontakte kontoret for at få slettet indhold i mails mv. via *Office 365*. Da der er tale om arbejdsredskaber har Brøndby Gymnasium ret til at slette indholdet på det udlånte udstyr. Det har man som medarbejder skrevet under på, da udstyret blev udleveret, jf. kvittering for udlevering af it-udstyr. Derfor

er det også en god ide, hvis medarbejderen løbende tager sikkerhedskopier af private billeder mv., som man ønsker at bevare i fremtiden.

- Hvis personoplysninger undtagelsesvist opbevares på USB-nøgle skal Brøndby Gymnasiums UBS-nøgler bruges. Som en ekstra sikkerhed kan USB-nøglen krypteres, hvilket let gøres ved at højre-klikke på USB-nøglen og vælge ”Slå Bit-locker til”. Herefter vælges en personlig adgangskode, som medarbejderen selv skal huske.

Sletning af dokumenter og mails mv., som indeholder personoplysninger

På Brøndby Gymnasium opbevares personoplysninger i de godkendte it-systemer, jf. Retningslinjer Godkendte IT systemer, og ikke andre steder.

I denne instruks kan du læse om, hvordan du sletter personoplysningerne fra et ”usikkert” system.

Det er vigtigt, din sletning af personoplysningerne fra det usikre system er det, man kalder ”effektiv”, dvs. at oplysningerne ikke kan gendannes i det usikre system, når du har udført sletterutinen.

Usikkert system	**Effektiv sletterutine**
Outlook (mails)	Mailen slettes (fra indbakken, sendt post eller ”slettet post”) ved at trykke ”delete” mens ”*shift*”-knappen holdes nede. Denne kommando sikrer, at mailen vil blive slettet permanent fra mailserveren efter 90 dage. I den 90-dages periode vil mailen kunne gendannes med ”Gendan”-funktionen i slettet post.[4]
Stifinder/skrivebord (Filer, fx word, excel, power point, mv.)	Filen slettes ved at højre-klikke på filen og vælge “slet” Vær opmærksom på, om computeren er indstillet til at slette permanent med det samme eller blot overføre filen til papirkurven. Hvis sidstnævnte er tilfældet, skal filen også slettes fra papirkurven for at være slettet effektivt.
USB-stick	Indholdet på USB’en slettes ved at stille musen på ”ekstern disk” i skærmbilledet ”denne PC”, højre-klikke og vælge ”formater”. ***BEMÆRK at denne kommando sletter ALT indhold på USB’en.***
Fysisk print	Fysiske dokumenter tilintetgøres ved makulering straks dokumentet har udtjent sit formål. Makulatorer står på kontoret ved Marianne.
Hjemmesiden	Karina administrerer hjemmesiden og kan slette billeder og kontaktinfo om medarbejdere i BG. Cache-filer fra søgemaskiner som fx Google, slettes som beskrevet her

[4] Slettede mails gemmes i 90 dage i back-up og kan i den periode gendannes med bistand fra Brøndby Gymnasiums IT