It-politik

Indledning

Tolne Efterskoles it-politik har til formål at sørge for at den daglige drift af it-systemerne forløber så problemfrit som muligt, og at skolens data er beskyttet mod utilsigtet indtræden i systemerne og ødelæggelse af data. Det er også vigtigt, at Tolne Efterskoles elever, forældre og samarbejdspartnere kan være sikre på, at deres oplysninger behandles sikkert og fortroligt.

It-politikken omfatter også retningslinjer for, hvordan du som medarbejder kan benytte web, mails osv. til private formål.

Sikkerhed og personlige oplysninger

Brugernavne og kodeord

Alle medarbejdere får tildelt brugernavne og kodeord til Tolne Efterskoles it-systemer. Kodeord er personlige, må ikke udleveres til andre og skal opbevares på et sikkert sted. Har du brug for at give andre adgang til dine data, fx i forbindelse med ferie, orlov eller tjenesterejser, skal du skifte kodeordet, når du vender tilbage. Kodeord/passwords må ikke gemmes på PC'en.

Lagring og backup af data

Skolens data skal altid lagres på de dertil indrettede fællesdrev og systemer. På den måde sikrer vi, at der er adgang til skolens data og at disse er sikret ved regelmæssige backups. Dette gælder også elevplaner og udtalelser. I arbejdet med skolens data på den ansattes IT-udstyr er det den ansattes ansvar at disse oplysninger ikke kan tilgås af andre end den ansatte og at oplysninger slettes, når arbejdet er afsluttet.

Lokale harddiske, USB-sticks og andre flytbare medier må du kun bruges til at gemme kopier af dokumenter og andre data på til brug for transport, og oplysninger skal være beskyttet af et kodeord. Private data kan du lagre på disse medier eller på dit eget netværksdrev. Hvis

Personregistrering

Tolne Efterskole lagrer personfølsomme oplysninger om elever, forældre og kontakter i overensstemmelse med Persondataloven og Datatilsynets forskrifter. I forbindelse med arbejdet med elevplaner og udtalelser er den ansatte ansvarlig for at slette alle oplysninger fra andre steder end skolens fælles drev og Intrasystem. Dette sikrer, at personfølsomme data KUN findes på førnævnte systemer.

Udarbejdelse af elevplanen skal foregå i VIGGO.

Brug af Tolne Efterskoles it-udstyr

Hardware og software

Pc'ere, mobiltelefoner og lignende udleveres normalt med al nødvendig software installeret. Dette indbefatter nødvendig sikkerhedssoftware i form af firewall, antivirus-programmer mv.

Disse programmer skal altid være aktive og opdateret, og du må derfor under ingen omstændigheder slå dem fra.

Hvor arbejdsmæssige hensyn gør det nødvendigt, kan du installere anden software, der er relevant for at du kan udføre dit arbejde tilfredsstillende. Det er en absolut forudsætning, at den installerede software overholder licensbetingelserne for anvendelsen. Piratkopier eller lignende må ikke findes på Tolne Efterskoles udstyr.

I de tilfælde, hvor skolens IT-udstyr benyttes hjemme skal det sikres, at ingen andre en den ansatte kan tilgå skolens data – evt. med oprettelse af særlig brugerprofil.

Internet og e-mails, sociale medier

På Tolne Efterskole kan du bruge e-mails, internet og sociale medier (Facebook, Twitter, LinkedIn osv.) til private formål, i det omfang tidsforbruget ikke påvirker udførelsen af dine daglige arbejdsopgaver i negativ retning.

Internettet og emails må kun benyttes til lovlige formål.

Vedrørende e-mails opfordrer Tolne Efterskole dig til altid at benytte dine egne mailadresser til private formål. Hvis du benytter din private mail i forbindelse med dit arbejde, må disse mails ikke indeholde personfølsomme oplysninger.

VIGGO kan bruges til beskeder med personfølsomme data – dog efter nøje overvejelse og kun til modtagere, der har med den involverede at gøre.

Twitter, Facebook og lignende

- Kontakt ledelsen på Tolne Efterskole, hvis du falder over en ophedet debat om Tolne Efterskole, i stedet for at selv at svare.

Forhold ved fratræden

Det er din pligt at fjerne private mails og dokumenter fra systemerne, hvis du fratræder din stilling i Tolne Efterskole. Hvis dette ikke kan lade sig gøre, vil Tolne Efterskole fjerne de private e-mails, og så vidt muligt overdrage disse til dig efterfølgende.

Ved brud på datasikkerhed

Opleves der tilfælde, hvor personfølsomme oplysninger utilsigtet er kommet i andres besiddelse følges nedenstående flow chart.