

---

## Instruks ved Borup Privatskole om behandling af personoplysninger og IT-sikkerhed

---

### Formål

Formålet med reglerne er at sikre, at skolens IT-systemer og anden dataregistrering håndteres med omtanke og på en måde, der sikrer tilgængelighed, integritet og fortrolighed og udelukkende udspringer af et velbegrunderet formål.

### Gyldighedsområde

Instruksen gælder alle der håndterer dokumenter eller anvender skolens IT-systemer, inklusive mobilt udstyr og hjemme-pc'ere, hvad enten disse anvendes arbejdsmæssigt eller privat og uanset hvor benyttelsen foregår.

### Overtrædelse

Hvis skolen konstaterer ulovlige håndtering, installationer eller filer, vil medarbejderen blive orienteret herom, hvorefter de vil blive afinstalleret eller slettet.

Ethvert misbrug eller overtrædelse af håndtering af data, analogt såvel som digitalt, kan medføre ændringer i ansættelsesforholdet og kan i gentagelsestilfælde eller i særligt grove tilfælde medføre opsigelse og/eller bortvisning.

---

## Alle 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 ALTID lukkes ned eller logges af efter endt brug.
- Computer og lignende udstyr (fx usb-stik, telefoner, harddiske eller tablets) skal opbevares på sikker vis og ikke må efterlades på offentlige steder eller på uovervågede/uaflåste steder på arbejdspladsen.
- Dokumenter (elektroniske såvel som analoge) der indeholder personoplysninger, skal altid opbevares på en måde, hvor kun personer, der har brug for oplysningerne, har adgang til dem.
- Elektroniske dokumenter og data indeholdende personoplysninger skal opbevares på udstyr udleveret af skolen – eksempelvis computer, telefon eller cloud-baserede systemer.
- Fysiske dokumenter og notater skal opbevares forsvarligt og i videst mulige omfang kun på skolen. Personfølsomme oplysninger opbevares udelukkende i det aflåste arkiv eller i klasseloggen (beskyttede elevdata)
- Computer og lignende udstyr er sikret med kode – se mere om sikkerhed nedenfor.
- Der logges udelukkende på PC'ere og IT-systemer med egen bruger og kode. Disse oplysninger må ikke udveksles med andre i eller udenfor organisationen.

## Skolens udstyr

Medarbejdere kan anvende skolens udstyr til private formål, så længe dette ikke strider mod lovgivningen og nærværende retningslinjer, skolens arv, renommé og værdier.

Der må ikke installeres ulovlige programmer, tilgås ulovlige sider eller lign. på udstyret.

Hvis medarbejderen anvender sin skole-emiladresse som kontaktsadresse ved køb over nettet, skal det sikres, at der ikke kan opstå tvivl om, hvorvidt skolen eller medarbejderen har foretaget købet.

### **Brug af mail og intranet**

Det er ikke tilladt at bruge sin private mail til arbejdsrelateret korrespondance som indeholder personoplysninger. Personoplysninger skal altid sendes via en sikker mail-løsning (gennem administrationen) eller via skolens intranet.

Hvis der modtages personoplysninger, som er tilsendt med ikke sikker mail, skal disse hurtigst muligt overføres til en sikker opbevaringsmetode og mailen slettes.

### **Brug af privat mobiltelefon**

Det er ikke tilladt at bruge privat mobiltelefon til sende beskeder indeholdende personoplysninger.

Såfremt der skal tages billeder eller video af elever og forældre skal disse billeder slettes efter brug eller arkivering på adgangskodesikrede platforme.

### **Brug af sociale medier**

Personoplysninger må aldrig deles på andres eller private sociale medier. Såfremt der skal deles billeder, videoer eller lignende skal det foregå på skolens officielle profiler og sider.

Portrætbilleder eller billeder af enkelte børn må aldrig lægges ud på sociale medier. Her må kun lægges situationsbilleder ud, evt. med flere børn.

Det forventes at alle ansatte på skolen, i forbindelse med at de identificerer sig som værende ansat på Borup Privatskole, repræsenterer skolen loyalt og professionelt.

### **Samtaler i det offentlige rum**

Medarbejdere skal være bevidste om, at andre kan se og høre, hvad de beskæftiger sig med, når de befinder sig i det offentlige rum, fx. på vej til og fra arbejde, på tjenesterejser eller til møder.

Det er ikke tilladt at føre samtaler i det offentlige rum, som gør det muligt for omkringværende at identificere de elever eller forældre det drejer sig om.

### **Sikkerhed**

IT-udstyr og papirer der indeholder eller giver adgang til følsomme oplysninger – herunder navnlig personfølsomme oplysninger skal altid håndteres under iagttagelse af passende sikkerhed. Det betyder for eksempel:

- At koder skal indeholde mindst 8 tegn
- At kodeord/passwords ikke genbruges til flere tjenester
- At koder skiftes med passende mellemrum – fx hver tredje måned
- At koder/passwords opbevares sikkert og adskilt fra udstyret – undgå, om muligt, at nedskrive kodeord/password
- At man ikke åbner mistænkelige mails og hjemmesider
- At mails indeholdende data med personfølsomme oplysninger, som ikke videresendes, medmindre det er strengt nødvendigt, fx i forbindelse med myndighedsbehandling – og at det i givet fald sker via sikker mail.

## Sikkerhedsbrud

Ansatte har pligt til, hurtigst muligt, at give skolens ledelse meddelelse om formodede eller konstaterede brud på ovenstående retningslinjer.

---

### Typer af personoplysninger:

#### **Almindelige oplysninger - Persondatalovens § 6**

*Navn, adresse, personnummer, skattemæssige oplysninger, bankoplysninger, uddannelse, påtaler, advarsler m.v.*

*Et ansættelsesbevis anses som accept af, at informationer der opgives også må anvendes og opbevares. Indmeldelsesblanket indeholder erklæring om samtykke til, som en samtykkeerklæring til behandling af oplysningerne.*

#### **Følsomme oplysninger - Persondatalovens § 7**

*Racemæssig eller etnisk baggrund, politisk eller religiøs overbevisning, fagforeningsmæssige tilhørsforhold, seksuelle forhold.*

*Følsomme oplysninger kræver **udtrykkeligt samtykke** før behandling og forudgående tilladelse fra Datatilsynet. I praksis vil det ofte være i forbindelse med indmeldelse af en elev, at eksempelvis oplysninger om religiøs overbevisning kan komme på tale. En skole bør generelt afholde sig fra at føre registre over den type oplysninger.*

#### **Private oplysninger – Persondatalovens § 8 stk. 4**

*Rent private forhold (eksempelvis alkoholmisbrug), personlighedstests, strafbare forhold.*

*Private oplysninger kræver **udtrykkeligt samtykke** medmindre de er nødvendige for at varetage en berettiget interesse, som klart overstiger hensynet til medarbejderen eller eleven. Registrering af private oplysninger kan være berettiget i ganske særlige tilfælde. Her kan det eksempelvis være ved mistanke om tyveri fra skolen eller overgreb på en eller flere elever. Er der en velbegrundet mistanke om, at en ansat stjæler fra skolen, vil denne type oplysninger ikke være omfattet af retten til indsigt i egne oplysninger da det kan skade en eventuel efterforskning.*

#### **Hjemmel**

*Det skal ud over ovenstående begrænsninger **ALTID** overvejes, om overlevering af oplysninger vedr. person bør ske. Det skal være nødvendigt for opgaveudførelsen.*