

Vår övergripande Dataskydd- och Integritetspolicy

För oss i Anton Utbildning och HVB är **personlig integritet viktig**.

Oavsett om du är medarbetare/elev/barn/vårdnadshavare är det viktigt att du skall känna dig trygg med hur dina personuppgifter behandlas. Vi eftersträvar en hög nivå av skydd för dina personuppgifter dvs att så få som möjligt behandlar dessa och att **rättslig grund** finns.

I rollen som skola/arbetsgivare behöver Antonskolan hantera dina personuppgifter. Det är bland annat för att kunna kommunicera med myndigheter, följa lagstiftning, kollektivavtal, samt för att du ska kunna använda de administrativa system som behövs i ditt arbete / din skolgång.

Du har rätt att ta del av vilka typer av personuppgifter som vi hanterar, för vilka ändamål, på vilken rättslig grund samt hur och hur länge vi sparar dessa och vem som ansvarar för att de förvaras på ett säkert sätt. Se vårt **GDPR-register** på hemsidan **antonutbildning.se**. Antonskolan kommer att radera dina personuppgifter när de inte längre behövs för det syfte de samlades in för. Personuppgifterna ska vara korrekta och uppdaterade och felaktiga personuppgifter raderas eller rättas utan dröjsmål vid kännedom om felaktighet.

I vissa fall när vi inte har laglig grund för att hantera dina personuppgifter, tex publicera en bild på sociala medier kan vi begära ditt **samtycke** för detta. Samtycke skall vara specifikt och tydligt för dig och går alltid att återkalla.

På Antonskolan har vi centrala tekniska lösningar för att höja säkerheten. Ta gärna del av vår **Policy för Digitala verktyg, E-mail, Google Docs**. Anton Utbildning AB är ansvarig för personuppgifter kopplade till alla medarbetare/barn/elever/vårdnadshavare. Det innebär att det är styrelsen i bolaget som är personuppgiftsansvarig.

Om du har frågor om hur dina personuppgifter hanteras kontakta i första hand Dataskyddsombudet via dataskyddsombudet@antonskolan.com eller din närmaste chef.

Detaljerad Dataskyddspolicy

Vårt dataskydd varierar med vilken information eller vilket system det gäller. Generellt har vi alltid brandväggar som ger ett visst skydd för angrepp som initieras utanför vårt gemensamma nätverk. Aktuella virusprogram installeras på samtliga datorer.

Alla våra centrala system och databaser säkerhetskopieras regelbundet, dock är det sällan som en enskild dator har automatisk backup. Istället rekommenderar vi medarbetare att lagra sitt arbete i vår molnlösning Google Drive eller på krypterad extern hårddisk / USB-minne.

Alla våra system kräver inloggning med användarnamn och lösenord. Dessutom har system med känslig eller verksamhetskritisk information ytterligare säkerhet i form av att man bara kan logga in inifrån vårt nätverk eller så kallad stark autentisering (bank-id eller 2-steps autentisering). Vi kan styra och låsa våra Googlekonton och datorer på distans ifall en dator skulle försvinna eller hamnar i orätta händer.