



IT-instruks og instruks om brugen af persondata for Værløse Golfklub (VGK)

Gældende fra: 19-03-2026

1. Generelt

I denne IT-instruks finder du de regler, der gælder for brugen af Værløse Golfklubs IT-systemer samt brugen af de persondata, som VGK giver dig adgang til i forbindelse med udførelse af opgaver for klubben. Persondata omfatter alle oplysninger, der kan knyttes til en person, fx navn, e-mail, telefonnummer, medlemsnummer, tøjstørrelse eller turneringsresultater.

VGK skal til enhver tid beskytte og værne om de persondata, vi modtager fra medlemmer, gæster, ansatte og samarbejdspartnere. Alle, der har adgang til persondata, skal følge denne instruks. Data må ikke kopieres eller videregives til personer uden legitim adgang.

2. Computere, telefoner og enheder der tilgår data

Alle enheder, der kan tilgå VGKs data, skal være beskyttet med password og/eller biometrisk login. Enheder skal låses, når de forlades, og kræve login igen efter maksimalt 15 minutters inaktivitet. Dette gælder også private enheder, der bruges til at læse eller opbevare mails eller dokumenter fra VGK.

3. Opbevaring af data / arkivering

3.1 Fysiske data

Fysiske persondata (noter, print, protokoller mv.) skal håndteres forsvarligt. Følsomme data og CPR-numre skal opbevares aflåst, når de ikke bruges.

3.2 Elektroniske data

Elektroniske persondata må kun opbevares i programmer, der er installeret eller godkendt af VGK.

Du må ikke installere egen software eller bruge uautoriserede fildelingstjenester.

3.2.1 Lokal opbevaring

Data på servere, NAS mv. skal være passwordbeskyttet og opbevaret i aflåste lokaler.



3.2.2 Online opbevaring

Online data skal tilgås via krypterede forbindelser (https).

Data må ikke opbevares på C-drev, USB-nøgler eller andre usikre medier.

4. Videregivelse af personoplysninger

Medlemsoplysninger må deles med andre medlemmer, når det har et sagligt formål, fx i klubblad eller på lukkede sider.

Offentliggørelse på åbne hjemmesider kræver samtykke.

Sponsorer, pro og café/restauration (hvis ikke ansat af klubben) må **ikke** modtage medlemsdata.

5. Brugernavne og passwords

- Undgå fælles brugerkonti.
 - Passwords skal være mindst 8 tegn og indeholde store/små bogstaver, tal og specialtegn.
 - Passwords til systemer med følsomme data skal skiftes hver 90. dag.
-

6. Sikkerhedsbrud

Alle brud eller mistanke om brud skal straks meldes til klubbens ledelse.

Dette inkluderer virus, mistænkelig adfærd på enheder eller mistænkelige mails.

7. Brug af e-mail

Alle typer persondata kan sendes på mail, hvis det er lovligt efter GDPR.

Følsomme oplysninger bør dog deles via sikre fildelingsløsninger.

Privat mail må kun bruges, hvis den er sikker og ikke deles med andre i husstanden.

8. Adgang til VGKs administrationssystemer

Adgange administreres af sekretariatet/bestyrelsen.

Adgang skal løbende tilpasses, så kun relevante personer har adgang.



9. Databehandling

9.1 Informationssøgning

Det er forbudt at søge efter persondata, der ikke er relevante for opgaven.

9.2 Eksport/udsendelse af data

- Del kun nødvendige data
- Gør modtager opmærksom på ansvar
- Følsomme data må kun deles med relevante myndigheder
- Brug sikre kanaler
- Brug BCC ved masseudsendelser

9.3 Sletning af data

Data skal slettes, når:

- de ikke længere er relevante
 - samtykke er trukket tilbage
 - lovgivning kræver det
-

10. Beredskab

Sikkerhedsbrud skal meldes til bestyrelsen/sekretariatet, som håndterer sagen.

11. Sanktionering

Overtrædelse af politikken kan medføre sanktioner fra skriftlig advarsel til eksklusion/afskedigelse.

Kvittering