

Policy för användning av digitala verktyg

Dokumentägare: IT-chef

IT och en ökad digitaliseringen ger oss nya möjligheter att nå våra mål, samtidigt ökar behovet av att vi använder digitala verktyg och digitala medier med gott omdöme. Syftet med denna policy är att beskriva hur vi som användare ska agera för att undvika risker för oss själva, våra deltagare eller AcadeMedia. Är du osäker? Ta kontakt med din verksamhets IT-chef eller AcadeMedia IT Support.

Denna policy omfattar medarbetare och konsulter inom AcadeMediakoncernen under arbetstid eller vid användning av företagets utrustning och/eller datakommunikation.

1. Privat användning

Privat användning är tillåten men ska inte inkräkta på arbetstid och ska göras med gott omdöme. Det är till exempel inte tillåtet att besöka webbplatser som förknippas med pornografi, rasism, nynazism eller liknande om det inte är professionellt motiverat. För att undvika oklarhet ska privata mejl inte skickas med företagsadressen som avsändare. Privata ljudfiler eller filmer ska inte lagras på företagets datorer eller lagringsytor då det ökar kostnader för bland annat backup, samma sak gäller lagring av fler än enstaka privata bilder.

2. Upphovsrättsskyddat material

Lagar och regler om upphovsrätt gäller även material som finns på internet. Det är inte tillåtet att använda information från internet på ett sätt som kränker upphovsrätten (t ex genom felaktig användning av bilder eller upp-/nedladdning av piratkopierat material).

3. Hantering av konton och lösenord

Lösenord är en allt viktigare del av vår digitala säkerhet och ska aldrig lämnas ut till annan person. Lösenord som används till AcadeMedias system får inte användas i något annat system eller tjänst då det kraftigt ökar risken för intrång. Om vi lämnar dator/platta/telefon utan övervakning ska den låsas eller stängas av så att obehörig åtkomst förhindras.

4. Känslig information

Känsliga personliga uppgifter eller annan känslig information ska alltid hanteras med försiktighet och endast lyftas ut ur, för dem avsedda, informationssystem om vi vet att hanteringen är säker. I dessa fall ska e-post användas minimalt och inte utanför koncernen. Känsliga dokument som skickas med e-post ska lösenordskyddas.

5. Installation av programvara



AcadeMedia

Om du installerar programvara som du varken fått via ramavtal eller enligt instruktion från AcadeMedia IT måste du vara helt säker på att den både är licensierad och inte innehåller skadlig kod. Om du är osäker ska du ta kontakt med AcadeMedia IT.

6. Övervakning och insyn

All lagrad information eller trafik kan under vissa förutsättningar komma att kontrolleras, exempelvis för att spåra hackerangrepp eller undersöka eventuella oegentligheter. Detta gäller även privat information eller användningshistorik som lagras på utrustning och system som tillhör AcadeMedia. Användare är i dessa fall skyldiga att efter förfrågan tillhandahålla nycklar för eventuell krypterad information.

Vill du veta mer om hur du skyddar dig och dina data läs mer på trygg.academedia.se.

Andra policyer och riktlinjer att känna till:

- [Riktlinjer för sociala medier](#) – anger både hur vi som enskilda individer och hur vi som organisation ska använda sociala medier.
- [Dataskyddspolicy](#) – anger hur vi som organisation ska hantera personuppgifter.
- [Informationssäkerhetspolicy](#) – anger hur vi som organisation ska arbeta för att nå en hög grad av tillgänglighet, konfidentialitet, riktighet och spårbarhet för vår information.

