Retningslinjer

For ScaleAQ-ansatte på nett og i sosiale medier

1. INNLEDNING

Sosiale medier som Facebook, Twitter og LinkedIn har blitt en viktig kommunikasjonskanal for både privatpersoner, bedrifter og offentlige institusjoner. For virksomhetene gir sosiale medier mange muligheter og noen utfordringer. For at vi alle skal ha en felles og gjensidig forståelse, har vi etablert noen retningslinjer og anbefalinger for bruk av sosiale medier – på vegne av selskapet og som privatperson.

2. SELSKAPET I SOSIALE MEDIER

2.1 Innledning

ScaleAQ er – og skal være – synlig i sosiale medier.

2.2 Hvem uttaler seg på vegne av selskapet?

Uttalelser og innlegg i sosiale medier på vegne av selskapet, skal kun gjøres av personer som er autorisert for dette.

2.3 Innholdet i kommunikasjonen

Ved all kommunikasjon i sosiale medier på vegne av selskapet skal følgende ivaretas:

- Verdiene våre skal være grunnlaget for all kommunikasjon.
- Vi skal fremstå med åpenhet og transparens.
- Vi skal alltid være ærlige og snakke sant.
- Vi skal opptre med aktsomhet, informativt og profesjonelt.

All kommunikasjon skal være innenfor lov, forskrift og avtaler. Vi skal:

- Respektere opphavsrettigheter og den enkeltes personvern.

- Unngå krenkelser av privatlivets fred.
- Ikke omtale sensitiv eller taushetsbelagt informasjon.

3. PRIVAT BRUK AV SOSIALE MEDIER

Privat bruk av sosiale medier er i utgangspunktet opp til den enkelte og tilhører den private sfære. Selskapet respekterer den enkeltes ytringsfrihet, *men ønsker også å minne om taushetsplikten (se arbeidsavtalen)*. På bakgrunn av vår virksomhet ønsker vi likevel å komme med noen anbefalinger og retningslinjer for privat bruk. Under finner du noen uformelle huskeregler som kan være greie å ta med seg.

3.1 Privat bruk og identitet

Tenk på ditt personlige digitale fotavtrykk. Det du selv publiserer i sosiale medier spres lett og forblir ofte synlig og søkbart i lang tid fremover, gjerne i flere år.

Unngå tvil og uklarhet om din identitet som kan bidra til unødige misforståelser. Skriv at du er ansatt i ScaleAQ om det er relevant. Du bør være åpen om at du jobber i ScaleAQ, og du må tydelig nevne at du uttaler deg som privatperson og med dine egne meninger. Hvis du ikke har avtalt noe annet med din leder representerer du deg selv, ikke selskapet. Skriv i førsteperson slik at det er tydelig at du uttaler deg som privatperson.

3.2 Lytt først

Alle sosiale medier har sin ytringskultur. Sett deg inn i og forstå spillereglene, oppfatningene og behovene til nettsamfunnet du adresserer før du engasjerer deg.

3.3 Ta stilling til hva du ønsker å ytre

Det er viktig å være bevisst hva man ønsker å ytre. Opptre fintfølende, informativt og profesjonelt. Husk at innholdet kan bli synlig for alle, selv om du publiserer innholdet innenfor en lukket krets. Ikke legg ut innhold som er egnet til å skade andres eller ditt eget omdømme.

Mange opplever at de angrer på det de legger ut (se www.slettmeg.no).

3.4 Unngå omtale av virksomhetsrelaterte forhold

Ta diskusjoner rundt utfordringer om forhold som angår jobben direkte med din leder – ikke på nettet. Når det gjelder jobben vår, skal vi ikke omtale:

- Virksomhetssensitive og taushetsbelagte tema.
- Kollegaene og lederne våre.

- Kunder, leverandører og samarbeidspartnere.
- Konkrete arbeidsoppgaver
- Vi skal ikke «sjekke inn» hos den bedriften vi besøker. Dette kan avhengig av det ærend vi har, faktisk være sensitiv informasjon.

3.5 Vær åpen

Fremstå med åpenhet og transparens i sosiale medier som i andre sammenhenger.

3.6 Respekter dine lesere

Del din kunnskap og dine erfaringer. Respekter andres standpunkter og unngå å bidra til konflikter.

3.7 Ta ansvar

Hvis du skulle komme til å trå feil, er det ofte en god strategi å innrømme feilen, eventuelt beklage og bidra til å rette den opp.

4. IKKE BLI LURT

Sosial manipulering utnytter menneskelig kontakt og sosiale evner for å få tak i eller påvirke informasjon. Forretningshemmeligheter, personopplysninger og informasjon om IT-systemer kan være verdifulle for andre og misbrukes til svindel eller kriminelle handlinger. Angriperen opptrer ofte liketil og respektabelt, og kan eksempelvis utgi seg for å være en reparatør, nyansatt eller driftsansvarlig. Han samler ofte informasjon fra flere hold, og bruker opplysninger fra den ene kilden til å bygge tillit hos den andre.

Generelle forholdsregler:

- Vær skeptisk til spontane forespørsler.
- Forsøk å få bekreftet personers identitet.
- Gi ikke ut informasjon som mottaker ikke har krav på.

Vær også kritisk til det som skrives på sosiale medier. Informasjonen er ikke alltid faktabasert, men enkeltpersoners meninger eller forståelse.