

## Heb oog voor privacy en informatieveiligheid

Als vrijwilliger werkt u soms met een computer, laptop of smartphone, maakt u soms gebruik van e-mail en beschikt u mogelijk over informatie van cliënten. Ga hier zorgvuldig mee om en bedenk van tevoren welke informatie u wel of niet kunt delen met anderen!

Verlies, diefstal, beschadiging, vernietiging, het niet beschikbaar zijn en/of ongeautoriseerd gebruik van (vertrouwelijke) informatie kan namelijk ernstige gevolgen hebben. Zo'n situatie kan negatief uitpakken voor de begeleiding en ondersteuning van onze cliënten. U kunt in strijd handelen met de wet, bijvoorbeeld de Algemene Verordening Gegevensbescherming (AVG) en de organisatie kan financiële schade lijden, bijvoorbeeld door uitval van systemen of vanwege herstelwerk, om nog maar niet te spreken over de eventuele imagoschade.

We willen u dan ook wijzen op onze 10 aandachtspunten voor privacybescherming en informatieveiligheid:

- Het vertrouwelijk omgaan met informatie is een verantwoordelijkheid van iedereen.
- Wees je tijdens je werk altijd bewust van 'meekijkers' en 'meeluisteraars'. Deel geen gevoelige informatie op sociale media of via openbare wifi-hotspots.
- Laat gegevens niet onbeheerd achter. Vergrendel je computerwerkplek (Windowstoets +L) en sluit kasten en lades af.
- Versnipper papieren met vertrouwelijke gegevens of gebruik de daarvoor bestemde 'Datazeke' papiercontainers.
- Zorg voor een 'leeg & schoon bureau, een blanco scherm'.
- Kies een goed wachtwoord en houd het geheim.
- E-mailen is in de basis niet veilig. Sta stil bij wat je schrijft, naar wie je schrijft, doorstuurt of als bijlage bijvoegt.
- Voorzie smartphones, tablets, laptops of USB-sticks van een pincode!
- Denk na over waar je vertrouwelijke informatie opslaat op de computer.
- Meld datalekken en computerincidenten zoals virussen, diefstal en verlies van apparatuur of verlies van je vrijwilligerspas bij je contactpersoon.