



## Veilig omgaan met informatie en het delen daarvan

**Informatie delen doe je dagelijks. In een gesprek, op papier, via e-mail, social media, WhatsApp of andere media. Veilig omgaan met het delen van informatie is in je werk essentieel. Die informatie gaat vaak direct of indirect over onze cliënten; mensen waarmee wij een vertrouwensrelatie hebben.**

**Dit protocol geeft richtlijnen hoe je zo veilig mogelijk met het delen van werkgerelateerde informatie kunt omgaan.**

Als professional ga je respectvol om met (privacy) gevoelige informatie - zie ook de Handreiking Privacy. Wees je bewust welke informatie je via welke weg gaat delen en bespreek dit eventueel met je collega's. Gebruik waar mogelijk de digitale voorzieningen die Philadelphia beschikbaar stelt om (privacy) gevoelige informatie te delen.

### Hoe pak je dit aan?

1. Bespreek met je collega's wat de richtlijnen zijn.
2. Vergrendel je apparatuur als je (even) weggaat en deel je inlognaam en wachtwoord niet met anderen.
3. Zorg dat je (privacy) gevoelige informatie, als je jouw werkplek verlaat, in een af te sluiten kast bewaard.
4. Bespreek met je leidinggevende als je vertrouwelijke informatie wilt delen met externen. Neem bij twijfel contact op met de Privacy Officer via [privacy@philadelphia.nl](mailto:privacy@philadelphia.nl). Als je cliëntinformatie wilt delen met externen bespreek dit met de cliënt/vertegenwoordiger. Deel dit alleen via Philadelphia e-mail (de mail wordt automatisch gecontroleerd en veilig verzonden).
5. Wanneer je op diverse werkplekken of thuis werkt, ga dan zorgvuldig om met het meenemen van informatie.
6. Bezoek, download of verspreid geen informatie die racistisch, discriminerend, pornografisch, beledigend of aanstootgevend is.
7. Wees voorzichtig met het openen van en het klikken op links in e-mails van verdachte afzenders en vooral met het openen van bestanden die je niet verwacht.
8. Gedraagt de computer, smartphone e.d. zich anders dan anders, neem dan contact op met de Servicedesk ICT.
9. Gebruik van communicatiemiddelen voor privé doeleinden tijdens je werk is beperkt toegestaan zolang het de kwaliteit en productiviteit van je werk niet negatief beïnvloedt.
10. Meld alle voorvallen waar je denkt dat er (per ongeluk) onverantwoord met informatie is omgegaan of gegevens in verkeerde handen terecht is gekomen (is datalek), bij de Servicedesk ICT. Dan kunnen we maatregelen treffen om erger te voorkomen.

### Wie heeft een taak?

- Alle medewerkers, leerlingen, stagiaires, uitzendkrachten, vrijwilligers, extern ingehuurd
- Leidinggevenden
- Security functionaris van het cluster
- Afdeling I&A
- Privacy Officer
- Information Security Officer

### Status

Dit protocol berust op de Algemene Verordening Gegevensbescherming (AVG) en de normen ISO27001/ NEN7510.

### Document eigenaar

Directeur Medewerkersbelang

### Voor het laatst aangepast

Januari 2026

### Evaluatietermijn

Ieder jaar

### Gerelateerde documenten

- Juridische bepalingen (bijlage)
- Handreiking Privacy
- Gedragscode
- Protocol Huisregels
- Protocol Veiligheid
- Protocol Ongewenste gebeurtenissen

### Welke middelen?

Dit protocol gaat over het delen van informatie met specifieke aandacht voor diverse platforms en middelen zoals: internet, PhilaNet, e-mail, social media, laptop, smartphone, iPad het gebruik van generatieve AI.

### Social media

Deze media zijn laagdrempelig; een bericht is zo geplaatst. Besef dat jouw berichten door veel mensen gelezen kunnen worden. Zie ook PhilaNet '[Social media inzetten](#)'.

## Servicedesk

[servicedesk.ict@philadelphia.nl](mailto:servicedesk.ict@philadelphia.nl)

of 033 - 760 22 22

Voor vragen over elektronisch communicatieverkeer.



“Je mag natuurlijk best tijdens een verjaardagsfeestje vertellen dat je een drukke dag hebt gehad op de locatie. Maar vertel niet dat cliënt Jan Schilder vandaag alweer een woede-uitbarsting heeft gehad en het meubilair in zijn kamer kapot heeft gemaakt. En laat niet op de tuintafel het cliëntdossier op je iPad openstaan terwijl je even bij de burens een kop thee drinkt.”

## Wist je dat? En tips

### Beveiliging digitale diensten

Philadelphia beveiligt haar digitale werkplek om zorgvuldig met (privacy) gevoelige informatie om te gaan. Denk hierbij aan gevoelige informatie rondom cliënten, medewerkers en organisatie. Deze beveiliging is ook nodig om te voldoen aan wetgeving op dit gebied.

### Gevoelige informatie

Als je (privacy) gevoelige informatie wilt delen doe dit dan mondeling of gebruik de Philadelphia digitale diensten om te communiceren. Gebruik de juiste systemen (ECD, Afas, InPlanning etc.) en bespreek met je collega's wanneer je wat gebruikt.

### Algemeen nieuws

Philadelphia gebruikt haar externe websites en haar social media kanalen voor algemeen nieuws dat met iedereen gedeeld mag worden.

### DigiContact

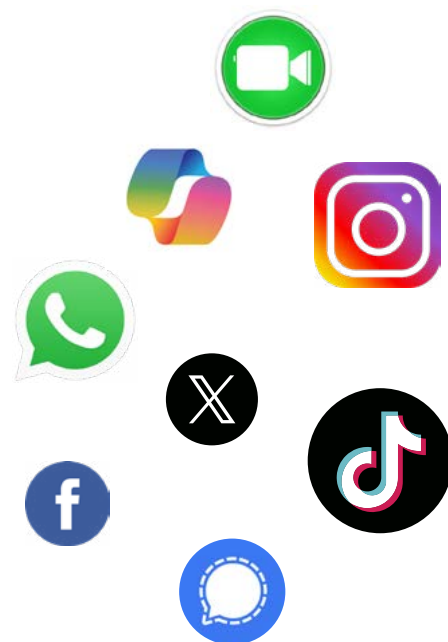
De medewerkers van DigiContact maken contact met een cliënt via beeldcommunicatie in een beveiligde omgeving.

### Facetime, Facebook, Instagram, Whatsapp, Signal, X, TikTok e.d.

Deze diensten zijn niet gericht op veilige communicatie en slaan gegevens vaak in het buitenland op. Hierdoor hebben wij geen controle over de data. Daarmee zijn ze ongeschikt voor het delen van (privacy) gevoelige informatie. Verwerk geen bedrijfs- of privacy gevoelige gegevens in generatieve AI-oplossingen zoals CoPilot en ChatGPT. Doe je dit toch? Dan brengt dit grote privacy risico's met zich mee. Gegevens worden gebruikt om modellen te trainen en kunnen in handen van onbevoegden vallen.

### Online vergaderen

Voor online vergaderen gebruiken we Teams. Via deze systemen kun je veilig online vergaderen. Meer informatie vind je op [PhilaNet](#).



## Controle

Wanneer Philadelphia het vermoeden heeft dat je in strijd met dit protocol handelt, dan heeft zij het recht om jouw gebruik van de diverse informatievoorzieningen te controleren. Je wordt wel van tevoren geïnformeerd over het doel van de controle en welke gegevens gecontroleerd worden. Afhankelijk van de ernst van het vermoeden kun je hangende het onderzoek geschorst of op non-actief gesteld worden.

Wanneer blijkt dat je in strijd met het protocol handelt kan Philadelphia arbeidsrechtelijke maatregelen treffen zoals: een officiële waarschuwing, een overplaatsing of ontslag (op staande voet). Dit zal afhankelijk zijn van de aard en de omvang van het handelen. Zie ook de [bijlage](#) met juridische bepalingen behorende bij dit protocol.

Heb je nog vragen  
en/of opmerkingen?

[Mail ons](#)