Veiligheidsplanner voor online activiteiten in sociaal werk

Philippe Bocklandt en Jo Van Hecke
Oktober 2015

Medewerkers in welzijns- en zorgorganisaties moeten als professionals mediawijs kunnen werken. Tot op zekere hoogte betrekken medewerkers van sociaal werkorganisaties zich ook op de mediawijsheid van hun doelgroep of cliënten.

Maar wat baten al die mediawijsheid van de gebruikers als de organisatie zelf niet mediawijs handelt:

- Welke inspanningen levert de organisatie om de steeds evoluerende nood aan mediawijsheid van haar medewerkers en cliënten bij te schaven?
- Welke hard- en software wordt voorzien?
- Welke afspraken over het communiceren op sociale netwerksites zijn er in de organisatie gemaakt? Is er een sociale mediabeleid?
- Wat zijn de spelregels over het opslaan en bewaren van online documenten en online cliëntgegevens?
- Enz.

Samen met je medewerkers bepalen aan welke mediawijze aspecten je als organisatie aandacht moet besteden, dat is het doel van de 'veiligheidsplanner voor activiteiten in sociaal werk'. Samen met Jo Van Hecke (Tonuso) werkten we dit planningsinstrument uit.

Voor begeleiding om te werken met deze veilgiheidsplanner kan je ook bij hen terecht:

- Jo Van Hecke (Tonuso) – jovanhecke@gmail.com
- Philippe Bocklandt (Arteveldehogeschool) – philippe.bocklandt@arteveldehs.be

Deze tekst maakt deel uit van 'Sociaal werk netwerkt online'
– een gps en tools om professioneel te communiceren op sociale netwerksites.
Dit materiaal kwam tot stand via 4 lerende netwerken met 50 beroepskrachten uit sociaal werkorganisaties.
Dit project werd opgezet door Cera en de Arteveldehogeschool.
Voor alle materiaal: www.sociaal-werk-netwerkt-online.be

Veiligheidsplanner voor online-activiteiten in sociaal werk

= op weg naar mediawijze organisaties =

Jo Van Hecke en Philippe Bocklandt

Waarop is deze veiligheidsplanner voor online-activiteiten in sociaal werk gebaseerd?

Deze 'veiligheidsplanner voor online-activiteiten in sociaal werk' in je organisatie is gebaseerd op materiaal van The South West Grid for Learning Trust[1]. Deze Engelse non-profitorganisatie wil scholen en andere organisaties ondersteunen i.v.m. veilig, door het organisatiebeleid ondersteund, online communiceren. Hun veiligheidsplanner werd voor jeugdzorgorganisaties in Vlaanderen vertaald en aangepast door Jo Van Hecke[2]. In zijn projecten (o.a. Medi@Train) van e-hulp-Vlaanderen werd en wordt deze safety-planner vaak gebruikt. Hij nam deze 'risicoanalyse en veiligheidsplanning' ook op in zijn publicatie[3].
De versie die voorligt werd 'vertaald' en verbreed naar het brede sociaal werk in het kader van het project 'Sociaal werk netwerkt online' waarbij 50 medewerkers uit sociaal werkorganisaties in vier lerende netwerken de mogelijkheden en beperkingen van het gebruik van sociale netwerksites verkenden. Dit project is een initiatief van Cera en de Arteveldehogeschool.

Wat wordt bedoeld met online-activiteiten in sociaal werk?

Ook in sociaal werk communiceren we meer en meer online: we raadplegen of beheren websites; we communiceren met collega's, cliënten of andere professionals via mail, chat, sociale netwerksites, …; we slaan allerlei data over onze cliënten en onze activiteiten online op; we gebruiken ondersteunende onlinetools zoals zelftesten, serious games, onlinedagboeken, … En die online-activiteiten zullen in de toekomst alleen maar toenemen.
Met online-activiteiten in sociaal werk bedoelen we dus alle communicatie vanuit de organisatie waarbij gebruik gemaakt wordt van ICT.

Waarom een veiligheidsplanner voor online-activiteiten?

Bij het off-line professioneel werken in sociaal werk wordt veel aandacht besteed aan de wijze waarop wordt gecommuniceerd en waarop de resultaten van deze communicatie in verslagen of dossiers wordt bewaard – zeker wanneer deze communicatie persoonlijke gegevens bevat.
Deze veiligheidplanner wil de risico's van de professionele online-communicatie in kaart brengen en de aandacht vergroten voor het systematisch verantwoord omgaan met de nieuwe ICT-mogelijkheden.
Deze veiligheidsplanner helpt om de sterktes en zwaktes van de online-activiteiten in je organisatie in kaart te brengen en te zoeken naar verbeteracties. Omdat de quickscan in samenwerking met de medewerkers (en mogelijks met de cliënten) gemaakt wordt, is het meteen een instrument om de mediawijsheid van deze betrokkenen te vergroten.

---

[1] The South West Grid for Learning Trust, Great Moor House, Bittern Road, Exeter, EX2 7FW - Tel: 01392 381371 Fax: 01392 381370 Email: enquiries@swgfl.org.uk
Website: http://www.swgfl.org.uk/
[2] Jo Van Hecke is medewerker van Tonuso en mede-coördinator van e-hulp-Vlaanderen.be
[3] Van Hecke, J. (red.) (2012) Internet als methodiek in de jeugdzorg – een extra taal. Leuven: Garant, p. 53-55.

Welke aspecten komen in deze veiligheidsplanner voor online-activiteiten in sociaal werkorganisaties aan bod?

Deze veiligheidsplanner bestaat inhoudelijk uit drie delen:

- Deel 1 focust op aandacht voor veilige online-activiteit vanuit *het organisatiebeleid*.
  Eindverantwoordelijkheid, regels, evaluatie/controle van de online-activiteit en het veilig online opslaan van persoonlijke data aan bod.
- Deel 2 focust op veilige online-activiteit door *de medewerkerkers* (en eventueel door *de cliënten*).
  In dit deel komen het melden van een gebrek aan mediawijsheid, evaluatie en bijsturing van mediawijsheid, aandacht voor mediawijsheid van cliënten en medewerkers aan bod. Er wordt specifiek ingezoomd op het omgaan met afbeeldingen, foto's, video's en persoonsgegevens door medewerkers en op het mediawijs gebruiken van sociale media.
  In dié organisaties die 'dagelijkse' begeleiding van cliënten verzorgen, kan mediawijsheid van die cliënten ook aan bod komen.
- Deel 3 focust op ICT-technologie.
  Aandacht voor veilige online communicatietools, veilige persoonlijke hard- en software van medewerkers, beveiliging van hard- en software staan hier centraal. Voor organisaties die 'dagelijkse' begeleiding van cliënten verzorgen komen daar veilige toegang tot het internet en monitoring van het internetgebruik van cliënten bij.

Hoe werkt deze veiligheidsplanner voor online-activiteiten in sociaal werkorganisaties?

Deze veiligheidsplanner bestaat uit drie fases:

- De veiligheidsplanner begint met een **quickscan** van de aandacht voor veiligheid van online-activiteiten in uw organisatie. Een risicoanalyse dus.
  Hoe ga je aan de slag met deze quickscan:
  - Bepaal het team dat deze quicksan invult. Dat kan elk team medewerkers van elke deelwerking zijn. Dat kan ook één team met een vertegenwoordiger van elke deelwerking zijn.
  - Elk teamlid krijgt de 'quickscan scorevragen' (3 blz.) en een 'scorekaart' (3 blz.) waarop voor elke vraag een code 'rood' – 'oranje' – 'groen' wordt aangekruist en de score gestaafd wordt met commentaar en argumenten.
- Alle individuele scorekaarten worden samengebracht op een gemeenschappelijke '**scorekaart veiligheidsplanner voor online-activiteiten'** die je daarvoor best op A3-formaat kopieert. Vanuit de bespreking van dit overzicht kom je tot een consensusscore met commentaar en argumenten.
- Op basis van deze consensusscore bepaal je als team concrete '**verbeteracties voor veiligheid van online-activiteiten'** zodat je volgende keer van 'rood' naar 'oranje', van 'oranje' naar 'groen' kan evolueren of score 'groen' kan behouden. Duid tevens aan wie voor deze actie verantwoordelijk zal zijn en welke timing je daarbij voor ogen hebt. Deze verbeteracties kunnen de basis zijn voor een volgend gesprek.

Het is zinvol om met regelmaat deze veiligheidsplanner opnieuw op te maken.

1 Quickscan van de veiligheid van online-activiteiten in sociaal werkorganisaties

Deel A: Scorevragen i.v.m. organisatiebeleid rond veiligheid van online-activiteiten					
Rubriek	**Vraag**	**ROOD**	**ORANJE**	**GROEN**	**Welke bewijzen kan je hiervoor gebruiken?**
Eind-verantwoordelijkheid voor de online-activiteit	Wie heeft de eind-verantwoordelijkheid voor de online-activiteit van de medewerkers (en ev. van cliënten)?	Niemand heeft de eindverantwoordelijkheid. Dus niemand weet wie eindverantwoordelijk is.	Iemand heeft de eindverantwoordelijkheid maar dit is niet door alle medewerkers gekend.	Iemand heeft de eindverantwoordelijkheid over de online-activiteit en dit is door iedereen gekend (en aanvaard).	Visie en doelen van de organisatie Werkplan Organigram Taakomschrijving Documenten reglement rond: ▪ Acceptabel gebruik ▪ Online regels ▪ E-safety ▪ Data beveiliging Verslagen vergaderingen Verslagen van ICT-acties
Regels over online-activiteit	Zijn er regels over de online-activiteit in de organisatie en zijn ze door medewerkers (en ev. door cliënten) gekend?	Er zijn geen specifieke regels over de online-activiteit.	Er zijn regels opgesteld maar die zijn niet door alle medewerkers (en ev. door cliënten) gekend.	Er is een duidelijke online strategie en er zijn duidelijke regels over de online-activiteit, gekend en aanvaard door medewerkers (en ev. door cliënten).	
Evaluatie/controle van de veiligheid van de online-activiteit	Wordt de veiligheid van de online-activiteit in de organisatie regelmatig geëvalueerd/gecontroleerd?	Er zijn geen regelmatige evaluaties/controles van de veiligheid van de online-activiteit.	Sommige online-activiteit wordt geëvalueerd/ gecontroleerd op veiligheid, maar er is nog nood aan verbetering.	Er zijn regelmatige evaluaties/controles en deze worden ook continu verbeterd en in vraag gesteld gezien de evolutie van de online-activiteiten.	
Veiligheid van het online opslaan van persoonlijke data	Worden persoonlijke data op een veilige manier online opgeslagen?	Er zijn zeer weinig maatregelen getroffen om persoonlijke data online te beschermen.	Er zijn fundamentele maatregelen getroffen om persoonlijke data online te beschermen en deze voldoen aan wettelijke eisen.	De veiligheidsmaatregelen i.v.m. het online opslaan van persoonlijke data zijn getroffen en begrepen door alle gebruikers. Dit heeft betrekking op zowel de bewaring van persoonlijke data, als op het minimaliseren van het risico van verlies of misbruik.	

Deel B: Scorevragen i.v.m. veilig online actief zijn door medewerkers (en ev. cliënten)					
Rubriek	**Omschrijving**	**ROOD**	**ORANJE**	**GROEN**	
(Aandacht voor mediawijsheid van cliënten)	Bestaat er aandacht voor het stimuleren van mediawijsheid van cliënten?	Er is geen aandacht voor, vorming, ondersteuning, begeleiding van cliënten i.v.m. mediawijsheid.	Er is materiaal beschikbaar om aandacht te besteden aan mediawijsheid van cliënten, maar deze wordt niet systematisch gebruikt.	Er zijn regelmatig acties om cliënten mediawijs te maken. Deze zijn ingepland en worden geëvalueerd en waar nodig bijgestuurd.	
Aandacht voor professioneel omgaan met online tools voor medewerkers	Bestaat er aandacht voor het professioneel gebruiken van online tools voor medewerkers?	Er is geen aandacht voor, vorming, ondersteuning, begeleiding van medewerkers i.v.m. het professioneel omgaan met online tools.	Er is materiaal en aandacht voor het professioneel omgaan met online tools voor medewerkers, maar dit wordt niet vaak gebruikt.	Er is op regelmatige basis aandacht en vorming voor en begeleiding van medewerkers i.v.m. het professioneel omgaan met online tools.	**Welke bewijzen kan je hiervoor gebruiken?** Rapportage, evaluatie en bijsturing i.v.m. mediawijsheid Incidentverslagen en consequenties i.v.m. omgaan met mediawijsheid Bronnen over mediawijsheid Procedures Vormingsprogramma's over mediawijsheid
Omgaan met digitale afbeeldingen, foto's, video's en persoonsgegevens door medewerkers	Wordt er specifiek aandacht besteed aan het omgaan met digitale afbeeldingen, foto's, video's en persoonsgegevens door medewerkers?	Er is geen duidelijk beleid rond het professioneel gebruik van digitale foto's, video's en persoonsgegevens door medewerkers.	Er is enige kennis i.v.m. digitale afbeeldingen, foto's en video, maar in de praktijk is dit nog niet altijd duidelijk en door iedereen gekend en toegepast.	Er is een duidelijke werkwijze over opslaan, gebruik, delen, publiceren, verspreiden van digitale beelden, foto's en video's. Deze wordt door alle medewerkers toegepast.	
Aandacht voor mediawijs gebruik van sociale media door medewerkers	Bestaat er aandacht voor het mediawijs gebruik van sociale media door medewerkers?	Er wordt in de organisatie geen aandacht besteed aan het mediawijs gebruik van sociale media door medewerkers.	(Sommige) medewerkers weten iets van mediawijs omgaan met sociale media, maar dit thema wordt niet systematisch aangepakt.	Alle professionele sociale mediaprofielen en –pagina's worden mediawijs gebruikt en dit wordt opgevolgd, bijgestuurd en geactualiseerd.	
Melding gebrek aan mediawijsheid	Is het duidelijk hoe en waar gebrek aan mediawijsheid kan gemeld worden?	Er is geen uitgewerkte procedure i.v.m. melden van een gebrek aan mediawijsheid.	Er is een procedure i.v.m. het melden van gebrek aan mediawijsheid, maar op het moment zelf moet nog veel overlegd worden.	Er is een manier om gebrek aan mediawijsheid te melden en deze is door de medewerkers (en ev. cliënten) gekend. Iedereen kan die toepassen.	
Evaluatie en bijsturing (ev. sanctionering)	Hoe wordt mediawijsheid geëvalueerd en gebrek aan mediawijsheid bijgestuurd (ev. gesanctioneerd)?	Er is geen gepaste evaluatie van mediawijsheid en indien nodig bijsturing (ev. sanctionering).	Er is een evaluatie van mediawijsheid en indien nodig bijsturing (ev. sanctionering) maar deze wordt niet consequent toegepast.	Medewerkers (en ev. cliënten) kennen de evaluatie van mediawijsheid en indien nodig bijsturing (ev. sanctionering). Positief online gedrag wordt beloond.	

Deel C: Scorevragen i.v.m. veilige ICT-technologie					
Rubriek	**Omschrijving**	**ROOD**	**ORANJE**	**GROEN**	
Online communicatietools	Gebruiken alle medewerkers veilige tools voor professionele online communicatie (mail, forum, chat, sociale netwerksites, blogs, …)?	Medewerkers weten niet duidelijk wat veilige tools voor professionele online communicatie zijn en stellen zich daar ook weinig of geen vragen over.	Medewerkers zijn geïnformeerd over veilige tools voor professionele online communicatie.	De organisatie beschikt over veilige tools voor professio-nele online communicatie. Alle medewerkers werken met déze tools en dit wordt door de organisatie geëvalueerd en waar nodig bijgestuurd.	**Welke bewijzen kan je hiervoor gebruiken?** Communicatieregels Een handboek of leidraad voor medewerkers Info op de website van de organisatie Documentjes met do's en don'ts over gebruik eigen hard- en software, wachtwoorden, … ICT security regels Webfiltering Interesse tonen tot leefwereld online en bespreekbaar maken. Een log bijhouden van de incidenten
Persoonlijke hard- en software	Wordt veilig gebruik van eigen devices (gsm's, smartphones, computers en andere hard en software) van de medewerkers ondersteund?	Veilig gebruik van persoonlijke online hard- en software van de medewerkers wordt niet ondersteund.	De voordelen en gevaren van het gebruiken van eigen online hard- en software van de medewerkers worden gecommuniceerd en er is enige begeleiding hierbij.	Het veilig gebruik van persoonlijke hard- en software van medewerkers wordt ondersteund. Dit wordt regelmatig herzien in het licht van de nieuwe technologieën.	
Beveiliging van hard- en software	Zijn de hard- en software die medewerkers gebruiken beschermd tegen virussen, hacking, enz. Zijn ze geüpdatet en beveiligd met een wachtwoord?	Hard- en software die medewerkers gebruiken zijn niet beschermd, of niet regelmatig geüpdatet. Paswoorden worden niet gebruikt.	Sommige toestellen hebben wel virusscanners en internet security, maar er is niet echt een beheerssysteem voor. Paswoorden worden wel gebruikt.	Hard- en software die medewerkers gebruiken worden regelmatig geüpdatet en beschermd tegen gevaren. Iedereen heeft een paswoord en wijzigt dit regelmatig.	
(Veilige toegang tot het internet voor cliënten)	Wordt er veilige toegang tot het internet gegarandeerd voor cliënten?	Een gebrek aan filtering op hard- en software of gebrek aan toezicht betekent dat de veilige toegang tot het internet voor cliënten niet kan worden gegarandeerd.	Filtering is geïnstalleerd op hard- en software. De toegang tot het internet gebeurt in het algemeen onder toezicht.	Een firewall wordt gebruikt om veilige toegang tot internet te garanderen ofwel een filtersysteem in combinatie met consequent toezicht.	

2 Scorekaart veiligheidsplanner online-activiteiten in sociaal werkorganisaties

Deel A	Score i.v.m. organisatiebeleid rond veiligheid van online-activiteiten				
Rubriek	ROOD	ORANJE	GROEN	commentaar	bronnen/verklaring
Eind-verantwoordelijkheid voor de online-activiteit					
Regels over online-activiteit					
Evaluatie/controle van de veiligheid van de online activiteit					
Veiligheid van het online opslaan van persoonlijke data					

Deel B	Score i.v.m. veilig online actief zijn door medewerkers (en ev. cliënten)				
Rubriek	ROOD	ORANJE	GROEN	commentaar	bronnen/verklaring
(Aandacht voor mediawijsheid van cliënten)					
Aandacht voor professioneel omgaan met online tools voor medewerkers					
Omgaan met digitale afbeeldingen, foto's, video's en persoonsgegevens door medewerkers					
Aandacht voor mediawijs gebruik van sociale media door medewerkers					
Melding gebrek aan mediawijsheid					
Evaluatie en bijsturing (ev. sanctionering)					

Deel C	Score i.v.m. veilige ICT-technologie				
Rubriek	ROOD	ORANJE	GROEN	commentaar	bronnen/verklaring
Online communicatietools					
Persoonlijke hard- en software					
Beveiliging van hard- en software					
(Veilige toegang tot het internet voor cliënten)					

3 Verbeteracties veiligheid online-activiteiten in sociaal werkorganisaties

Deel A	**Verbeteracties i.v.m. organisatiebeleid rond veiligheid van online-activiteiten**		
Rubriek	Concrete verbeteracties	Door wie	Tegen wanneer
Eind-verantwoordelijkheid voor de online-activiteit			
Regels over online-activiteit			
Evaluatie/controle van de veiligheid van de online activiteit			
Veiligheid van het online opslaan van persoonlijke data			

Deel B	Verbeteracties i.v.m. veilig online actief zijn door medewerkers (en ev. cliënten)		
Rubriek	Concrete verbeteracties	Door wie	Tegen wanneer
(Aandacht voor mediawijsheid van cliënten)			
Aandacht voor professioneel omgaan met online tools voor medewerkers			
Omgaan met digitale afbeeldingen, foto's, video's en persoonsgegevens door medewerkers			
Aandacht voor mediawijs gebruik van sociale media door medewerkers			
Melding gebrek aan mediawijsheid			
Evaluatie en bijsturing (ev. sanctionering)			

Deel C	Verbeteracties i.v.m. veilige ICT-technologie		
Rubriek	Concrete verbeteracties	Door wie	Tegen wanneer
Online communicatietools			
Persoonlijke hard- en software			
Beveiliging van hard- en software			
(Veilige toegang tot het internet voor cliënten)			

‘Sociaal werk netwerkt online’ bevat veel meer

Deze tekst maakt deel uit van de website www.sociaal-werk-netwerkt-online.be
Deze website bevat een gps en tools voor beroepskrachten uit sociaal werkorganisaties die professioneel willen communiceren op sociale netwerksites:

Een e-book

Een gps naar sociale netwerksites met tips en aanbevelingen voor beroepskrachten van organisaties in welzijnswerk en gezondheidszorg.

14 teksten rond verdiepende invalshoeken

- Technische werken
- Werken met beelden
- Spelregels van sociale media
- Monitoren van sociale media

- Sociale mediabeleid
- Deontologie
- Samenwerken
- Communicatiemix

- Doel, doelgroep en stijl
- Plannen van info
- Interactie
- Boosten van info

- Mediawijze cliënten en medewerkers
- Mediawijze organisatie

Ondersteunende tools

checklists | filmpjes | afwegingen | inspirerende praktijken | stappenplan/ infographics | links | literatuur

Dit project kwam tot stand dankzij de medewerking en inbreng van meer dan 50 sociaal werkers.
Dit project is een initiatief van

artevelde hogeschool
cera samen investeren in welvaart en welzijn