Protocol Sociale Media SSgN
Mei 2026

Inleiding

Sociale media en digitale communicatie maken onlosmakelijk deel uit van het dagelijks leven van leerlingen en medewerkers van de SSgN. Platforms zoals WhatsApp, Instagram, Snapchat en TikTok bieden kansen voor contact, informatie-uitwisseling en betrokkenheid, maar kunnen binnen de schoolcontext ook leiden tot misverstanden, grensoverschrijdend gedrag, privacyproblemen of onveiligheid.

Deze regeling ‘sociale media’ is opgesteld op basis van het Protocol ICT en sociale media van de stichting voCampus**.** Dat protocol vormt het formele en juridische kader voor het gebruik van ICT en sociale media binnen alle scholen van de stichting. De voorliggende regeling is daarvan een schoolspecifieke uitwerking, afgestemd op de praktijk, cultuur en ervaringen binnen de SSgN.

Dit document biedt:

- Duidelijke en eenduidige afspraken over wat wel en niet is toegestaan;
- Helderheid over professionele grenzen in online contact tussen medewerkers en leerlingen;
- Houvast bij incidenten op social media, zoals online pesten, het delen van beelden of het gebruik van privékanalen;
- Een gezamenlijk referentiekader, zodat iedereen weet wat er van hem of haar verwacht wordt.

Niet om te controleren of te wantrouwen, maar om veilig, professioneel en pedagogisch verantwoord handelen te ondersteunen. Het helpt om verwachtingen expliciet te maken, incidenten te voorkomen en, wanneer dat nodig is, zorgvuldig en consistent op te treden.

Regeling en afspraken SSgN

Veilig werken, privacy beschermen en professioneel blijven

De volgende punten uit het protocol vragen om specifieke vertaling naar de dagelijkse praktijk van de SSgN:

Communicatie en Professionaliteit

- Formeel contact tussen werknemers en/of ouders verloopt altijd via de door school beschikbaar gestelde middelen (schoolmail en MS Teams).
- Digitale communicatie en contact met leerlingen verloopt uitsluitend via de door school beschikbaar gestelde middelen (schoolmail en MS Teams).
  Waarom? Dit voorkomt misverstanden, beschermt je tegen integriteitskwesties en waarborgt de privacy van de leerling.
- Stuur schoolmail niet automatisch door naar je privémail.
- Mail je naar externen (bijv. ouders of instanties) met persoonsgegevens? Zet bij het mailen naar meerdere personen de adressen altijd alleen in de BCC.

Privacy en Beeldmateriaal

- Maak geen foto's of video's van personeel of leerlingen zonder hun expliciete toestemming.
- Gebruik geen USB-sticks of externe harde schijf voor school, tenzij door school geleverd.
- Opslag en verwerking van data mag *niet* via commerciële privédiensten zoals Gmail, Hotmail of Dropbox verlopen.
- Lees je schoolmail op je eigen telefoon? Zorg dat je telefoon beveiligd is met een toegangscode of vingerafdruk/gezichtsherkenning.

Beveiliging en Apparatuur

- Deel nooit je wachtwoord en vergrendel bij het verlaten van een werkplek de computer of laptop (Windows-toets + L).
- Diefstal, verlies van apparatuur of een vermoeden van een datalek moet direct (binnen 72 uur) gemeld worden bij de leidinggevende en de privacy verantwoordelijke.

Gedrag online:

- Plaats nooit foto's of filmpjes van leerlingen of collega's op sociale media zonder hun uitdrukkelijke schriftelijke toestemming.
- Laat je op sociale media niet negatief uit over de school, collega's of leerlingen. Deel geen vertrouwelijke informatie.

WEL DOEN (Do's)	NIET DOEN (Don'ts)
Communiceren via Teams, Outlook, Magister, Zermelo	Appen met leerlingen via Whatsapp of andere kanalen
Scherm vergrendelen (Win + L) bij weglopen	Ingelogd lokaal verlaten 'voor heel even'
Opslaan in de school-cloud (OneDrive)	Toetsen en/of schoolgegevens opslaan op een privé USB of laptop
Reputatieschade online direct melden	Denken 'het valt wel mee' en niets zeggen
Toestemming vragen voor een foto	Zomaar een klassenfoto op sociale media zetten.

Escalatieladder

De escalatieladder is een hulpmiddel om gestructureerd en zorgvuldig te handelen bij signalen of zorgen. Het geeft stapsgewijs aan wanneer en hoe je handelt, wie je daarbij betrekt en welke acties passend zijn per niveau. Zo ondersteunt de ladder bij het maken van afgewogen keuzes en het waarborgen van de juiste zorg of ondersteuning.

Fase 1

Signaleren en bespreken
Doel: informeren, bewustwording, herhaling voorkomen, herstel en gezamenlijke oplossing

- Gesprek met betrokkene(n) (leerling/ouder/medewerker) ter kennisgeving
- Afspraken maken en eventueel schriftelijk vastleggen.
- Indien nodig: melding bij mentor, teamleider, directie of pestcoördinator

Fase 2

Formele waarschuwing en monitoring
Doel: gedrag bijsturen, escalatie voorkomen, grenzen stellen en/of veiligheid waarborgen

- Herstelgesprek of bemiddeling met betrokkene(n) (leerling/ouder/medewerker).
- Schriftelijke waarschuwing en vastlegging in personeels- of leerlingdossier.
- Mogelijke inzet van intern en/of externe expert (vertrouwenspersoon, pestcoördinator)

Fase 3

Herstelgerichte interventie of disciplinaire maatregel
Doel: uitvoeren van vervolgstappen conform het social-mediaprotocol.

- Gesprek met betrokkene(n) (leerling/ouder/medewerker) ter informatie.
- Concrete maatregel (schorsing of aangepaste afspraken)
- In uiterste gevallen: verwijdering, officiële klacht, ontslagtraject (medewerker).

Wanneer welke fase?

Fase 1:

- Overtreding is niet bewust en niet gericht op het bewust aanbrengen van schade voor het slachtoffer. Het is een eenmalige actie met geringe impact voor getroffene(n). Schade is eenvoudig te herstellen.

Fase 2:

- Overtreding is bewust ingezet om slachtoffer te schaden. Actie heeft grote impact op getroffene(n). Herstel zonder blijvende schade is lastig.
- Het is de tweede overtreding, waarbij de eerste viel onder fase 1.

Fase 3:

- Overtreding is een actie die oproept of aanzet tot geweld en/of sabotage.
- De actie is wijdverspreid over de digitale kanalen en zorgt voor veel negatieve opschudding binnen (en buiten) school.
- Overtreding is doelbewust ingezet om slachtoffer(s) (blijvende) schade te berokkenen.
- Het is de tweede overtreding, waarbij de eerste viel onder fase 2.
- Het is de derde overtreding, waarbij de eerste twee vielen onder fase 1 en 2.

Voor de volledige juridische kaders verwijzen wij naar het officiële 'Protocol ICT en social media voCampus' dat te vinden is op de website van voCampus.