

Gebruik sociale media in het onderwijs

Handvatten voor verantwoord gebruik



Colofon

Dit document is bedoeld als handreiking voor onderwijsinstellingen voor het gebruik van sociale media.

Bestemd voor

Dit document is bestemd voor alle onderwijsinstellingen in het MBO, HO en WO.

Samenstelling en beheer

Dit document is tot stand gekomen via de werkgroep 'Advies gebruik sociale media' in samenwerking met het Privacy Expertise Centrum van SURF. Het beheer van dit document berust bij SURF. Het past bij VW.01 (Verantwoording) van het Toetsingskader Privacy.

Speciale dank gaat uit naar de werkgroepleden:

- Joyce van der Klugt, Hogeschool Rotterdam;
- Gerrit Haakma, Firda
- Ralph Kronieger, Nimeto;
- Wladimir Mufty, SURF
- Alexandra van Straaten, SURF
- Helma De Boer, SURF
- Peter Vermeijs, MBO Raad

Licentie

Dit document is verstrekt onder de creative commons-licentie [CC BY](#) 4.0 International (naamsvermelding). SURF aanvaardt geen aansprakelijkheid voor enig gebruik/toepassing van dit document.

Versiebeheer – VW.01

Versie	Door	Datum	Toelichting/wijziging
1.0	Werkgroep en PEC	18-09-2025	Initieel document

Inhoudsopgave

Bestemd voor	2
Samenstelling en beheer	2
1 Inleiding	4
1.1 Uitgangspunten	4
1.2 Context	4
2 Advies AP over commerciële inzet sociale media	5
2.1 Kern van het AP-advies aan onderwijsinstellingen	5
2.2 Duidelijke afspraken en transparantie	5
3 Uitvoerbaarheid het AP-advies	6
3.1 Geen afspraken met leveranciers van sociale media-apps te maken	6
3.2 Grondslag 'toestemming' niet bruikbaar	6
4 Kanttekeningen/opmerkingen	7
4.1 Boetes 7	
4.2 Beheer en informatiemanagement	7
4.3 Hoge risico's	7
5 Commercieel gebruik van sociale media door onderwijsinstellingen	8
5.1 Doelen commercieel gebruik van sociale media	8
5.2 Wettelijke kaders: privacy en gegevensbescherming	8
5.3 Ethische grondslagen en verantwoordelijkheid	9
5.4 Regels en richtlijnen voor commercieel gebruik van sociale media	9
5.5 Toezicht en handhaving	9
6 Gebruik onder voorwaarden – handelingsperspectief	10
6.1 Verantwoorde oplossingen	10
6.2 Eerste aanzet tot handelingsperspectief	11
6.3 Voorrang vragen SURF Vendor Compliance	11
6.4 Ethiek en (commerciële) inzet sociale media	11
6.4.1 Sociale media gebruiken op basis van ethische grondslagen	11
6.4.2 Regels en richtlijnen	12
7 Advies	13
Bijlage - Alternatieven	14

1 Inleiding

In de zomer van 2024 heeft de Autoriteit Persoonsgegevens (AP) een [advies¹](#) gepubliceerd over het inzetten van sociale media door onderwijsinstellingen. Dit advies volgt op een voorafgaande raadpleging (VR) door een onderwijsinstelling, naar aanleiding van een Data Protection Impact Assessment (DPIA) met betrekking tot TikTok. Een VR is vereist wanneer uit een DPIA een hoog, niet te mitigeren risico voortvloeit – in dit geval de onbeheersbare gevolgen van gegevensoverdracht. De AP heeft haar advies hierover verstrekt en besloten dit niet op het specifieke platform TikTok te richten, maar op alle sociale media die door onderwijsinstellingen kunnen worden gebruikt. Het advies richt zich in de basis op gebruik voor marketing- en communicatiedoelstellingen (ook wel ‘commercieel gebruik’) door organisaties, bijvoorbeeld voor het werven van studenten. Door de aard van het advies strekt het zich inhoudelijk echter ook uit over educatief gebruik.

Dit advies van de AP is de aanleiding geweest om dit rapport met handvatten voor de onderwijssector te schrijven als handreiking voor onderwijsinstellingen.

1.1 Uitgangspunten

Onderwijsorganisaties moeten transparant zijn over het gebruik van persoonsgegevens, de rechten van studenten (en ouders) respecteren en duidelijke richtlijnen vaststellen voor het gebruik van sociale media, zowel voor promotionele als educatieve doeleinden.

De sociale media spelen een belangrijke rol in het aantrekken van studenten bij het mbo, ho en wo, omdat studenten hier al actief zijn. Het commerciële gebruik van sociale media door onderwijsinstellingen moet echter zorgvuldig worden afgestemd op de geldende privacywetgeving, zoals de AVG, ethische normen en de educatieve doelen van de onderwijsinstelling. Het uiteindelijke doel is om een veilige, transparante en ethisch verantwoorde omgeving te waarborgen waarin commerciële belangen niet ten koste gaan van de onderwijskundige integriteit en het welzijn van de studenten.

1.2 Context

Er zijn twee vormen van gebruik van sociale media te onderscheiden:

- Commercieel gebruik – medewerkers gebruiken apps voor marketing- en communicatiedoelstellingen. Hier gaat het over persoonsgegevens van zowel de personen die de advertentie of content te zien krijgen als van de werknemer die de app in het werk gebruikt.
- Educatief gebruik – leraren en/of studenten gebruiken apps voor onderwijsdoelstellingen. Hier gaat het over persoonsgegevens van de medewerker en van de student.

Het advies van de AP gaat specifiek over het commerciële gebruik, maar dat schetst een vergelijkbare situatie voor educatief gebruik.

¹ Rechtstreekse link naar [het advies](#)

2 Advies AP over commerciële inzet sociale media

In het advies gaat de AP uitgebreid in op de problemen met de verzameling en gebruik van persoonsgegevens voor commerciële doeleinden via sociale media en de bijbehorende risico's.

2.1 Kern van het AP-advies aan onderwijsinstellingen

De kern van het advies is:

“Onderwijsinstellingen mogen sociale media alleen inzetten als zij duidelijke afspraken maken met socialemediabedrijven over wat er met de gegevens van studenten en docenten gebeurt. Lukt het niet om zulke afspraken te maken? Dan kan een onderwijsinstelling het betreffende sociale medium beter niet gebruiken.”

In het advies geeft de AP aan dat organisaties de volgende punten moeten regelen voordat ze sociale media inzetten:

- **Verantwoordelijkheid** - Het moet helder zijn welke partij (gezamenlijk) verantwoordelijk is voor welk deel van de verwerking. Gezamenlijke verwerkingsverantwoordelijken moeten afspraken maken onder andere over hoe er met de rechten van betrokkenen wordt omgegaan. Dit moet transparant worden gecommuniceerd.
- **Bewaartermijnen** - Daar waar de onderwijsinstelling (gezamenlijk) verwerkingsverantwoordelijk is, is de organisatie ook verantwoordelijk voor de naleving van de bewaartermijnen, ook voor de naleving daarvan door de andere partij.
- **Passende maatregelen** – De verwerking van persoonsgegevens wordt initieel door de onderwijsinstelling in gang gezet. Als er onvoldoende passende maatregelen kunnen worden getroffen is doorgifte van persoonsgegevens niet toegestaan.
- **Toestemming** – Afhankelijk van de inzet van het sociale medium is het van belang dat de betrokkene toestemming geeft (vrij, specifiek en geïnformeerd).

2.2 Duidelijke afspraken en transparantie

De AP adviseert onderwijsinstellingen dus om eerst duidelijke afspraken met de platforms te maken over het gebruik van deze gegevens, bijvoorbeeld met betrekking tot:

- het gebruik voor andere doeleinden;
- de overdracht naar landen buiten de Europese Economische Ruimte (EER), dus buiten de reikwijdte van de Algemene Verordening Gegevensbescherming (AVG) - de onderwijsinstelling moet controleren of er sprake is van een (geldig) adequaatheidsbesluit of van Standard Contractual Clauses (SCC's) die aan de vereisten voldoen. Als hier geen sprake van is, kan de doorgifte niet plaatsvinden.
- contractuele borging van naleving van de bewaartermijnen voor zover er sprake is van een gezamenlijke verwerkingsverantwoordelijkheid.

Als een onderwijsinstelling dit nalaat, kan dit volgens het advies strijdig zijn met de AVG.

De AP merkt ook op dat het SURF gelukt is om vergelijkbare afspraken te maken met Google en Microsoft. Onderwijsorganisaties en/of SURF maken zulke afspraken ook met leveranciers, maar juist met socialemediabedrijven als leveranciers is het niet eenvoudig onderhandelen over de

verwerking van persoonsgegevens omdat zij minder belang hebben bij het aanpassen van hun beleid. Hoewel dit proces tijdrovend kan zijn, zoals gebleken uit eerdere afspraken tussen onderwijskoepels SURF en SIVON met Google, is het volgens de AP niet onmogelijk. Echter het is zeker voor een individuele onderwijsinstelling moeilijk zo niet onmogelijk om de vereiste afspraken te maken.

De (gezamenlijke) verwerkingsverantwoordelijken moeten ook de betrokkenen transparant en grondig informeren over de gevolgen van het verwerken van hun gegevens op het sociale mediaplatform op het moment dat een betrokkene om toestemming wordt gevraagd.

3 Uitvoerbaarheid het AP-advies

3.1 Geen afspraken met leveranciers van sociale media-apps te maken

Volgens de AP mogen onderwijsinstellingen dus geen sociale media-apps inzetten, tenzij zij concrete afspraken maken met de platforms. In de praktijk lijkt dat echter niet realistisch. Het hangt daarnaast ook af van hoe je de sociale media-apps gebruikt. Vergelijk het bijvoorbeeld ook met een AI-tool. Als je geen afspraken kunt maken, blijven de mogelijkheden voor gebruik beperkt, maar de knelpunten lossen niet op.

Onderwijsorganisaties zijn verantwoordelijk voor het waarborgen en naleven van de AVG. Hieronder valt ook de bescherming van privacy van (aankomende) studenten, ouders en medewerkers. Socialemediabedrijven behouden het recht voor om gegevens voor hun eigen doelen te gebruiken, AI te trainen en te verkopen². Deze dataverzamelingen door derden, mogelijk ook buiten de EU, zijn zeer ongewenst. Het is echter moeilijk schriftelijke afspraken te maken over de gezamenlijke verwerkingsverantwoordelijkheid. Als een onderwijsinstelling toch besluit sociale media in te zetten, moeten zij de (ongunstige) servicevoorwaarden accepteren. Daardoor zijn er geen goede afspraken over het gebruik en de vereiste privacywaarborgen van het sociale medium mogelijk.

3.2 Grondslag 'toestemming' niet bruikbaar

Voor onderwijsinstellingen lijkt het inzetten van sociale media voor marketing- en communicatiedoeleinden alleen mogelijk op basis van de grondslag 'toestemming'. Dat houdt in dat betrokkenen hiervoor toestemming moeten geven. Het advies gaat in op alle vereisten van op de juiste manier toestemming vragen en verkrijgen. De nadruk ligt op vrijwillige toestemming en de mogelijkheid om toestemming in te trekken.

Rechtsgeldige toestemming moet vrijelijk, ondubbelzinnig, geïnformeerd en specifiek worden gegeven. Hierbij moet een organisatie duidelijk toelichten voor welke specifieke verwerking toestemming wordt gevraagd. Om een betrokkene goed te kunnen informeren, moet de instelling zelf ook goed begrijpen welke verwerkingen er precies plaatsvinden, ook als deze verwerkingen plaatsvinden bij een derde partij waarvoor er nog (gezamenlijke) verwerkingsverantwoordelijkheid is.

² Meta heeft een opt-out regeling aangeboden voor AI trainen op Instagram en Facebook

De toestemming wordt geacht niet vrijelijk te zijn gegeven als er geen afzonderlijke toestemming voor de verschillende verwerkingen van persoonsgegevens kan worden gegeven. Daarbij komt dat in afhankelijkheidsrelaties – zoals een werknemer ten opzichte van een werkgever³, of een student ten opzichte van de onderwijsinstelling – vaak moet worden aangenomen dat de afhankelijke partij de toestemming niet in vrijheid heeft kunnen geven vanwege mogelijke negatieve gevolgen bij weigeren van deze toestemming. Voor personen jonger dan 16 jaar geldt bovendien dat zij toestemming moeten hebben van de persoon die de ouderlijke verantwoordelijkheid draagt.

Verder moet de organisatie kunnen aantonen dat toestemming is verkregen en moet het voor de betrokkene duidelijk zijn dat de gegeven toestemming op elk moment kan worden ingetrokken. Het verwerken van persoonsgegevens op grond van uitdrukkelijke toestemming van betrokkenen is in de praktijk behoorlijk lastig, juist omdat toestemming op ieder moment kan worden ingetrokken.

4 Kanttekeningen/opmerkingen

4.1 Boetes

De afgelopen jaren zijn tientallen zware Europese boetes opgelegd en gepubliceerd wegens onwettig gebruik en het delen van data via sociale media-apps. Het aantal waarschuwingen ligt veel hoger dan het aantal boetes doet vermoeden.

4.2 Beheer en informatiemanagement

Het goed beheren, koppelen en integreren van sociale media-apps met de bestaande informatie- en communicatiesystemen is moeilijk en vereist inzet van de organisatie. Meerdere systemen gebruiken voor hetzelfde doel is minder efficiënt en verhoogt het risico op een datalek.

4.3 Hoge risico's

De hoge risico's door het gebruik van sociale media ontstaan onder andere door:

- Verzamelen van persoonsgegevens via de app en het ongevraagd delen met moederbedrijven en eventuele andere partijen voor commerciële doeleinden, zonder transparantie.
- Geen grip op het gebruik van de gegevens door de (gezamenlijke) verwerkingsverantwoordelijke, ook voor wat betreft bewaartermijnen en voorzien in de rechten van betrokkenen
- Er kunnen geen wettelijke verplichte schriftelijke afspraken met socialemediabedrijven worden gemaakt.
- De grondslag 'toestemming' is praktisch niet werkbaar en geen solide basis voor veilige en betrouwbare communicatie.
- Grotere beheerlast; complexe informatiemanagement verhoogt risico (op een datalek).
- Groter risico op hoge boetes.

³ Ook het verkrijgen van rechtsgeldige toestemming van een medewerker of docent kan problematisch zijn. Dit speelt vooral bij medewerkers die – bij gebrek aan een telefoon verstrekt door de organisatie – gebruik moeten maken van hun eigen (privé) telefoon(nummer) voor sociale media-apps die de organisatie inzet.

5 Commercieel gebruik van sociale media door onderwijsinstellingen

Het commercieel gebruik van sociale media door onderwijsinstellingen is een complex onderwerp, vooral wanneer het in verband wordt gebracht met privacywetgeving, ethiek en verantwoord gebruik van technologie. Onderwijsorganisaties hebben steeds meer manieren om sociale media te gebruiken voor promotie, communicatie met studenten en ouders/wettelijk vertegenwoordigers, fondsenwervingscampagnes en zelfs educatieve doeleinden. Dit vereist een zorgvuldige afweging van de ethische en wettelijke kaders, zoals de Algemene Verordening Gegevensbescherming (AVG) en de AI Act (Artificial Intelligence Act).

5.1 Doelen commercieel gebruik van sociale media

Onderwijsorganisaties kunnen sociale media inzetten voor verschillende commerciële doeleinden, zoals:

- Promotie van onderwijsinstellingactiviteiten (open dagen, evenementen, etc.).
- Studiekeizers voor het maken van een goede studiekeuze.
- Het onder de aandacht brengen van het onderwijsaanbod en de beleving van andere studenten te delen.
- Fondsenwervingscampagnes voor onderwijsinstellingprojecten of infrastructuurverbeteringen.
- Een groter bereik onder de doelgroep te realiseren.
- Partnerships en sponsorschappen met bedrijven die onderwijs gerelateerde producten of diensten aanbieden.

Hoewel deze commerciële activiteiten waardevol zijn voor de onderwijsinstelling, het zorgvuldig reguleren ervan is belangrijk om te voldoen aan het ethisch beleid en de wettelijke verplichtingen van een organisatie.

5.2 Wettelijke kaders: privacy en gegevensbescherming

Wanneer onderwijsinstellingen sociale media gebruiken voor commerciële doeleinden, moeten ze de privacy van hun studenten en personeel waarborgen. Dit is niet alleen essentieel om te voldoen aan de AVG, maar ook om het vertrouwen van de onderwijsinstelling te behouden.

Concreet betekent dit:

- **Transparantie** over welke gegevens worden verzameld (bijvoorbeeld bij het gebruik van online formulieren of het bijhouden van interacties via sociale media).
- **Toestemming** van betrokkenen (vooral ouders en leerlingen) voordat persoonlijke gegevens, zoals afbeeldingen, video's of persoonsgegevens, worden gedeeld.
- **Minimale gegevensverwerking**: Alleen de strikt noodzakelijke gegevens mogen worden verzameld en gebruikt.
- **Commerciële partnerschappen en bedrijven**: wanneer een onderwijsinstelling samenwerkt met commerciële partners op het gebied van sociale media, moet er rekening mee worden gehouden dat partners vaak toegang hebben tot data die ze mogelijk voor marketingdoeleinden willen gebruiken. Onderwijsorganisaties moeten duidelijk

communiceren welke gegevens worden gedeeld en waarom, ook over het gebruik van gerichte advertenties (targeted advertising) of sponsoring door externe bedrijven.

5.3 Ethische grondslagen en verantwoordelijkheid

Het is van belang dat commerciële activiteiten niet ten koste gaan van het onderwijskundige doel van de onderwijsinstelling. Onderwijsorganisaties moeten ervoor zorgen dat commerciële berichten of advertenties geen afbreuk doen aan de educatieve ervaring van de studenten. Dit kan bijvoorbeeld door:

- **Grenzen stellen** aan commerciële berichten die de educatieve inhoud verstoren of afleiden.
- **Integratie van commerciële inhoud** die daadwerkelijk bijdraagt aan het onderwijs, zoals samenwerkingen met technologiebedrijven voor educatieve tools.
- **Verantwoordelijkheid in inzet in het gebruik van AI en data**
Met de opkomst van AI en data-analysetools wordt het steeds gemakkelijker om gedetailleerde profielen van studenten en hun ouders te creëren. Het gebruik van AI-gedreven advertenties of het verwerken van persoonsgegevens in AI-modellen moet altijd ethisch verantwoord gebeuren
- **Eerlijkheid en transparantie** over het gebruik van AI om gepersonaliseerde content of advertenties te leveren.

5.4 Regels en richtlijnen voor commercieel gebruik van sociale media

Onderwijsorganisatiebeleid en gedragsregels

Onderwijsorganisaties moeten duidelijke interne richtlijnen hebben over het commerciële gebruik van sociale media, inclusief:

- **Beperkingen op promoties** – hoe en wanneer mogen commerciële berichten worden gedeeld, bijvoorbeeld enkel tijdens specifieke evenementen of campagnes.
- **Verbod op commerciële invloeden in lesmateriaal** - onderwijsinstellingen moeten voorkomen dat commerciële partners invloed uitoefenen op het onderwijsaanbod of het curriculum.
- **Verantwoorde Interactie met sociale media** - onderwijsinstellingen dienen ervoor te zorgen dat commerciële activiteiten niet leiden tot ongewenste effecten, zoals **cyberpesten**, **online manipulatie** of het creëren van **onnodige sociale druk** bij studenten. Dit kan door het stellen van grenzen aan het gebruik van sociale media tijdens lestijd en het stimuleren van digitale geletterdheid.

5.5 Toezicht en handhaving

Er moet toezicht worden gehouden op het commerciële gebruik van sociale media, ook intern (door de onderwijsinstelling zelf, bijvoorbeeld via een onafhankelijke FG):

- **Interne controlemechanismen** moeten garanderen dat de onderwijsinstelling zich houdt aan de ethische en wettelijke richtlijnen bij het gebruik van sociale media.
- **Handhaving van sancties** bij misbruik of schending van privacyregels of ethische standaarden, bijvoorbeeld bij het onterecht delen van persoonsgegevens of het plaatsen van ongepaste commerciële content.

6 Gebruik onder voorwaarden – handelingsperspectief

6.1 Verantwoorde oplossingen

Technologische ontwikkelingen volgen elkaar snel op en organisaties of onderwijsinstellingen sturen hier vaak niet direct op. De maatschappij omarmt de techniek, waardoor organisaties hiermee geconfronteerd worden. Wanneer systemen die studenten verwachten, minder geschikt blijken vanwege privacywetgeving, is het soms noodzakelijk ze toch te gebruiken. Het onderwijs gebruikt sociale media voor communicatie en begeleiding van studenten. In gevallen waarin bijvoorbeeld sociale media nodig is om bereikbaar te blijven voor studenten, is een verbod op gebruik niet wenselijk, maar goede afspraken helpen om risico's te beperken.

Om verantwoorde oplossingen voor het gebruik van sociale media te vinden, zoekt men handvatten. Hierbij kan de aanpak begeleidingsethiek van prof. dr. ir Peter-Paul Verbeek en Daniël Tijink (zie afbeelding hieronder) behulpzaam zijn. Deze aanpak stelt dat technologische ontwikkelingen onvermijdelijk zijn en handelingsperspectieven moeten worden opgesteld.



Aanpak begeleidingsethiek, ontwikkeld voor het Platform voor de InformatieSamenleving (ECP)

Dit wordt gedaan door eerst de technologie in context te plaatsen, bijvoorbeeld TikTok door een communicatieafdeling. Men bespreekt actoren, waarden en effecten en neemt handelingsopties onder de loep: aanpassing of verbod van de technologie, alternatieven, of aanpassing van de omgeving. Een andere optie is verandering in het gebruik, zoals bewustwording en toestemming vragen bij het inzetten van een sociaal medium.

Een individuele aanpak door organisaties is mogelijk minder effectief gezien het advies van de AP. De focus ligt op overkoepelende organisaties zoals de MBO Raad, SURF, Vereniging Hogescholen en UNL. Ook zij moeten een proces doorlopen om gedegen adviezen te formuleren. De AP suggereert dat afspraken met aanbieders mogelijk zijn. SURF en Kennisnet hebben eerder afspraken gemaakt met Google. Het probleem is echter de benodigde tijd, terwijl dit voor het onderwijs urgent is.

Een voorstel kan zijn om een keuzemodel voor sociale media op te stellen, waarin do's en don'ts van belangrijke platforms worden opgenomen of naar alternatieven wordt verwezen, zie bijlage 1. Dit kan door specialisten samen te brengen of via een bredere aanpak waarbij begeleidingsethiek als handvat dient.

6.2 Eerste aanzet tot handelingsperspectief

1. Het maken van een algemene inventarisatie van gebruikte sociale media met de voor- en nadelen en risico's. Hoe wordt het platform ingezet, hoe omvangrijk is het gebruik en welke privacy-issues kunnen we identificeren.
2. Het maken van een lijst van eisen/gebruiksvoorwaarden rondom privacy aan de apps die in het algemeen van toepassing zijn (los van de functionaliteit van de app) en aangeven wat het gevolg is als aan bepaalde voorwaarden niet kan worden voldaan. Dit kan variëren tot een advies om zo'n platform helemaal niet te gebruiken of alleen onderdelen daarvan wel of niet te gebruiken of te bekijken of er aanvullende maatregelen kunnen genomen. Die maatregelen kunnen bijvoorbeeld awareness of het vragen van toestemming zijn.
3. Het formuleren van mitigerende maatregelen om risico's te beperken voor bepaalde functionaliteit (bijvoorbeeld voor chatapps: schakel de toegang tot het adresboek van de smartphone uit als om toegang wordt gevraagd, gebruik beheerde telefoons, maak heldere afspraken over wat wel en niet in een app mag worden gedeeld).
4. Een lijst van alternatieven aanreiken voor de functionaliteit van de gewenste sociale media.

6.3 Voorrang vragen SURF Vendor Compliance

Het onderwijs in Nederland heeft bij SURF een prioriteitenlijstje ingeleverd over de gewenste landelijke DPIA's op grote en veelgebruikte applicaties. Mogelijk moeten de veelgebruikte socialemediaplatforms vanwege het urgente probleem boven aan deze lijst komen.

6.4 Ethiek en (commerciële) inzet sociale media

6.4.1 Sociale media gebruiken op basis van ethische grondslagen

Ethisch beleid rond het gebruik van sociale media, AVG en de AI Act richt zich op het waarborgen van privacy, transparantie, en verantwoordelijkheid bij het gebruik van persoonsgegevens, gevoelige bedrijfsgegevens en inzet van kunstmatige intelligentie (AI).

Dergelijke beleid helpt het evenwicht te bewaren tussen innovatie en bescherming van individuele rechten. Dit is essentieel in een digitaal tijdperk waarin technologieën zoals sociale media en AI een steeds grotere rol spelen in ons dagelijks leven.

Dit omvat onder andere:

1. **Privacybescherming** - Het waarborgen van de privacy van gebruikersgegevens door middel van duidelijke voorwaarden voor gegevensverwerking en expliciete toestemming van gebruikers.
2. **Transparantie** - Het verstrekken van heldere informatie over hoe gegevens worden verzameld, gebruikt en gedeeld, zodat gebruikers geïnformeerde keuzes kunnen maken.
3. **Verantwoorde AI** - Het bevorderen van verantwoordelijk gebruik van AI-technologieën met inachtneming van ethische principes zoals eerlijkheid, rechtvaardigheid en non-discriminatie.
4. **Toezicht en handhaving** - Het handhaven van regels en normen om ervoor te zorgen dat bedrijven en organisaties zich houden aan deze ethische principes, met passende sancties voor niet-naleving.

6.4.2 Regels en richtlijnen

Het gebruik van sociale media door studenten op een onderwijsinstelling valt onder verschillende regels en richtlijnen, die zowel op nationaal als op onderwijsinstellingniveau kunnen verschillen. Onderwijsorganisaties hanteren een mix van wettelijke regels, ethische richtlijnen, en eigen beleid om het gebruik van sociale media door studenten te reguleren. Het doel is om een veilige leeromgeving te waarborgen, privacy te beschermen en studenten bewust te maken van de impact van hun gedrag online.

De belangrijkste regels en aandachtspunten zijn:

1. Privacy & AVG (Algemene Verordening Gegevensbescherming)

Onderwijsorganisaties moeten voldoen aan de AVG en mogen geen persoonlijke gegevens van studenten verzamelen of delen via sociale media zonder toestemming. Docenten en onderwijsinstellingen mogen geen privé-informatie van studenten delen via sociale media zonder toestemming.

2. Onderwijsorganisatiebeleid & gedragsregels

Veel onderwijsinstellingen hebben een eigen socialemediabeleid waarin staat wanneer en hoe studenten sociale media mogen gebruiken. De onderwijsinstelling kan bijvoorbeeld verbieden dat studenten tijdens het volgen van onderwijs platforms zoals Instagram, TikTok of Snapchat gebruiken. Ook kan de organisatie studenten verbieden in de context van het onderwijs persoonsgegevens van anderen, zoals foto's of video's, online te plaatsen zonder toestemming. Studenten mogen geen andere studenten, docenten of medewerkers kwetsen, pesten of beledigen via sociale media. Cyberpesten kan leiden tot disciplinaire maatregelen en in ernstige gevallen zelfs juridische consequenties. Onderwijsorganisaties kunnen sancties opleggen bij ongepast gebruik, zoals cyberpesten of het verspreiden van schadelijke inhoud.

3. Verantwoord gebruik & digitale geletterdheid

Onderwijsorganisaties stimuleren verantwoord en kritisch gebruik van sociale media. Dit kan via lessen over digitale geletterdheid, AVG, AI-geletterdheid en mediawijsheid. Studenten worden aangemoedigd om bewust om te gaan met hun digitale voetafdruk en nepnieuws te herkennen.

4. AI & sociale media in onderwijs

AI-gegenereerde content en deepfakes worden steeds populairder. Studenten moeten leren om deze kritisch te benaderen en deze niet te delen of gebruiken. Gebruik van AI-tools zoals ChatGPT en andere generatieve AI kan worden beperkt of juist worden geïntegreerd in het onderwijs. Hier moet vooraf het beleid duidelijkheid bieden via het curriculum of exameneisen.

7 Advies

Het belangrijkste is dat de organisatie grip heeft op haar eigen verwerkingen. Medewerkers moeten daarom in eerste instantie altijd de apps gebruiken die de organisatie faciliteert. Hierop is de juiste bescherming geregeld. Denk aan Teams-chat voor communicatie.

Op basis van het AP-advies versus de behoefte en de uitvoerbaarheid volgen onderstaande handvatten.

Het advies is om het gebruik van sociale media niet in te zetten voor commerciële doeleinden van de organisatie en het gebruik ervan voor educatieve doeleinden door studenten niet af te dwingen vanwege de verschillende privacy- en complianceproblemen.

Om te kunnen voorzien in de behoefte in het (beperkt) gebruik van bepaalde sociale media, geven we de volgende aanbevelingen:

1. Bevorder het gebruik van veilige alternatieven (zie bijlage 1) waar die beschikbaar zijn (bijvoorbeeld Signal in plaats van WhatsApp).
2. Gebruik veilige manieren voor marketing- en communicatiedoelen, bijvoorbeeld Piwik in plaats van Google Analytics. Gebruik geen trackingpixels in verband met de verdere verwerking door big tech.
3. Gebruik bij voorkeur door AI gegenereerde foto's of zorg voor een quitclaim als foto's van medewerkers of studenten voor promotiedoelstellingen worden gebruikt.
4. Maak heldere afspraken over of en op welke manier sociale media-apps kunnen worden gebruikt. Er mogen geen gevoelige gegevens worden uitgewisseld.
5. Educatief gebruik: laat studenten zelf kiezen met welke sociale media-apps ze bepaalde opdrachten willen maken/inleveren, maar zorg ervoor dat de organisatie in ieder geval een veilige, beheerde optie faciliteert.
6. Wordt een bepaalde functionaliteit niet door de organisatie aangeboden en wil een docent een bepaalde sociale media-app daarvoor inzetten, dan moeten er duidelijke voorschriften zijn of en hoe zo'n tool gebruikt mag/moet worden.
7. Gebruik voor commerciële doeleinden geen sociale media-apps die de organisatie niet faciliteert.
8. Sta – als dat in lijn is met de regels - medewerkers toe (maar verplicht nooit) om bijvoorbeeld WhatsApp te gebruiken in communicatie met studenten. Stel dus regels vast over of en welke informatie via zo'n route wel en niet mag worden gecommuniceerd.
9. Er mag geen uitwisseling zijn tussen beheerde en niet-beheerde sociale media-apps.
10. Faseer het gebruik van onveilige sociale media-apps (big tech) voor commerciële of educatieve doeleinden van de organisatie uit.

Bijlage - Alternatieven

Er zijn verschillende Europese alternatieven. Je kunt deze vinden op onder andere:

- [European-alternatives.eu](https://european-alternatives.eu)
- [Tweakers](https://tweakers.net)
- opensourcealternative.to