Protocol ICT en social media

Vaststelling CvB : 06-12-2021
Instemming GMR : 09-12-2021

Inleiding

Computers, internet, e-mail en social media zijn niet meer weg te denken uit onze maatschappij en (dus) ook niet uit het onderwijs. Om goed onderwijs te kunnen verzorgen is het noodzakelijk om gebruik te maken van de mogelijkheden die computers, internet, e-mail en social media bieden.

Het gebruik van computers, internet, e-mail en social media brengt echter ook risico's met zich. En er gelden ook wettelijke regels. Van eenieder wordt daarom verwacht dat men computers, internet, e-mail en social media verantwoord en overeenkomstig de wettelijke regels gebruikt.

In dit protocol wordt vastgelegd hoe binnen @voCampus dient te worden omgegaan met computers, internet, e-mail en social media, conform de visie van waaruit we werken binnen @voCampus. Regels, afspraken en geëxpliciteerde gedragsverwachtingen over dat ICT-gebruik zijn noodzakelijk omdat verkeerd of onverantwoord gebruik grote negatieve gevolgen kan hebben.

Waar in dit protocol in de mannelijke vorm wordt gesproken, wordt tevens de vrouwelijke vorm bedoeld.

Preambule

Doelstelling Protocol ICT en social media

In dit protocol zijn normen en uitgangspunten vastgelegd ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
- het tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
- de bescherming van privacygevoelige informatie waaronder persoonsgegevens van het schoolbestuur, haar medewerkers, leerlingen en hun ouders en daarmee het beschermen van de privacy en veiligheid van alle betrokkenen;
- de bescherming van vertrouwelijke informatie van het schoolbestuur, zijn medewerkers, leerlingen en hun ouders;
- het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen;
- de bescherming van de intellectuele eigendomsrechten van het schoolbestuur en derden;
- het voorkomen van negatieve publiciteit;
- kosten- en capaciteitsbeheersing.

Persoonsgegevens en Privacywetgeving

Persoonsgegevens verdienen bijzondere aandacht. Dit zijn gegevens die een persoon betreffen én waardoor een persoon geïdentificeerd of identificeerbaar is. Denk hierbij aan naamgegevens, emailadressen maar ook telefoonnummers van zowel collega's als leerlingen en ouders van leerlingen.

De privacywetgeving verplicht elk individu om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat @voCampus schriftelijk afspraken maakt met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk). @voCampus heeft een Functionaris voor Gegevensbescherming (FG) aangesteld. Deze communiceert intern de gedragsregels die horen bij het verwerken van persoonsgegevens. Persoonsgegevens moeten altijd met uiterste zorgvuldigheid verwerkt en gedeeld worden.

Als persoonsgegevens toegankelijk en of inzichtelijk zijn voor personen, die geen toegang behoren hebben tot deze gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en @voCampus. Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt @voCampus afspraken over:

- de verwerking en verspreiding van vertrouwelijke- en persoonsgegevens. Er worden niet meer gegevens verwerkt dan noodzakelijk om het doel te bereiken,
- de uitwisseling van gegevens, waarbij aan de ontvanger wordt aangegeven wat de ontvanger wel of niet mag doen met de gegevens,
- opslag en verspreiding van gegevens, waarbij alléén gebruik gemaakt wordt van door @voCampus beschikbaar gestelde middelen.

Vertrouwelijkheid

@voCampus werkt in beginsel op basis van vertrouwen en gaat uit van de professionaliteit van haar medewerkers. Van medewerkers van @voCampus en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bijvoorbeeld personeelsdossiers, vertrouwelijke enquêtegegevens, zorgdossiers et cetera, wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. Dat zij de privacywetgeving hanteren en op geen enkele wijze informatie, waarvan redelijkerwijze kan worden aangenomen dat deze vertrouwelijk of privacygevoelig is, zonder toestemming van betrokkene of leidinggevende te gebruiken en/of naar buiten te brengen.

Controle op het gebruik van ICT en ICT-middelen

De regels voor controle op het gebruik van ICT en ICT-middelen zijn een verplichting die voortkomt uit de privacywetgeving rondom de verwerking van persoonsgegevens. @voCampus zal dan ook de controle en handhaving van deze regels conform de privacywetgeving en het algemene arbeidsrechtelijk kader uitvoeren. Hierbij is het uitgangspunt een goede balans tussen verantwoord gebruik van ICT en ICT-middelen en de bescherming van de privacy van medewerkers op de werkplek. Gegevens worden alleen verzameld en gebruikt voor deze doelen.

Algemene normen

Iedere medewerker voldoet aan de volgende algemene normen voor 'zorgvuldigheid' (niet uitputtend):

- Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht.
- Voorkom het lekken van interne en vertrouwelijke informatie.
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen. (beveiligingsmaatregelen).
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild (bijvoorbeeld door jailbreaks).
- Meld een beveiligingsincident of datalek, een diefstal of verlies van ICT-middelen onmiddellijk na constatering zo spoedig mogelijk, maar altijd binnen 72 uur bij je direct leidinggevende en de privacyverantwoordelijke op school en Functionaris Gegevensbescherming (FG) via m.schoonus@vocampus.nl of 06 – 13 68 32 83.

Dit protocol staat in relatie tot andere documenten zoals de gedrags- en integriteitscode, het privacyreglement, het datalekprotocol, de klachtenregeling. Het protocol is een openbaar document dat medewerkers, ouders, leerlingen, externe relaties en andere belanghebbenden kunnen inzien via de websites van @voCampus en haar scholen.

Protocol ICT en social media

Artikel 1 Definities

a. **ICT**: Informatie- en communicatietechnologie.
b. **ICT-apparatuur**: apparatuur waarmee gebruik kan worden gemaakt van ICT dan wel dit gebruik ondersteunt.
c. **ICT-dienst**: de dienst van @voCampus die belast is met het goed functioneren van ICT.
d. **Schoolnetwerk**: het ICT-netwerk van @voCampus.
e. **Social media**: alle huidige en toekomstige online platformen waarvan de gebruikers de inhoud verzorgen.
f. **Gebruiker**: eenieder die ten behoeve van @voCampus werkzaamheden verricht (medewerkers, tijdelijk aangestelde externe deskundigen, stagiairs en vrijwilligers, leden van de Raad van Toezicht, etc.), of onderwijs volgt (leerlingen) en die gebruik maakt of kan maken van door @voCampus aan hem ter beschikking gestelde ICT-apparatuur of door @voCampus aan hem verleende toegang tot ICT.
g. **Gebruik**: het gebruik van ICT-apparatuur en/of ICT van @voCampus, ongeacht of deze binnen of buiten de (school)organisatie plaatsvindt.
h. **Bevoegd gezag**: de bestuurder van @voCampus.
i. **Schoolleiding**: de rector of directeur van de school die door @voCampus in stand wordt gehouden;
j. **Schoolmail**: de specifiek voor en door @voCampus beschikbaar gestelde e-maildienst.
k. **Gedragscode**: de Gedragscode van @voCampus.
l. **Privacyreglement**: het Privacyreglement van @voCampus.
m. **Schooldata**: alle data die school-gerelateerd zijn.
n. **Persoonsgegevens**: informatie die ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.
o. **AVG**: Algemene Verordening Gegevensbescherming en de daarop gebaseerde regelgeving.

Artikel 2 Toepasselijkheid protocol

2.1 Dit protocol geldt voor alle gebruikers.
2.2 Iedere nieuwe gebruiker wordt gewezen op de toepasselijkheid en vindplaats van dit protocol.
2.3 Het bevoegd gezag en de schoolleiding dragen er zorg voor dat de inhoud van dit protocol bij alle gebruikers genoegzaam bekend is.

Artikel 3 Gebruik van ICT-apparatuur

3.1 De gebruiker dient steeds zorgvuldig om te gaan met de door @voCampus verstrekte ICT-apparatuur, zodanig dat deze niet beschadigd of verloren raakt of gestolen wordt. In geval van schade, verlies, diefstal of bij het ontbreken van onderdelen, dient de gebruiker hiervan direct melding te doen bij zijn direct- leidinggevende.

3.2 Het is de gebruiker niet toegestaan om door @voCampus verstrekte ICT-apparatuur aan derden in gebruik te geven.
3.3 Buiten het koppelen en ontkoppelen van een laptop aan een dockingstation door een medewerker is uitsluitend de ICT-dienst bevoegd om apparatuur te (ont)koppelen, te verplaatsen of aan te sluiten aan het schoolnetwerk of aan apparatuur die aan het schoolnetwerk verbonden is. Mogelijke uitzonderingen hierop komen tot stand in overleg met de ICT-dienst.
3.4 Externe datadragers (USB-stick, externe harde schijf e.d.) van leerlingen en medewerkers mogen nooit aan apparatuur van school worden gekoppeld.
3.5 Het is niet toegestaan om persoonsgegevens of beeldmateriaal op te slaan op externe datadragers zoals een USB-stick of externe harde schijf. Indien een uitzondering hierop noodzakelijk lijkt, kan deze alleen in overleg met en met goedkeuring van de ICT-dienst gerealiseerd worden.
3.6 Het is niet toegestaan om schooldata op te slaan op externe datadragers zoals een USB-stick of externe harde schijf. Mogelijke uitzonderingen hierop komen tot stand in overleg met de ICT-dienst.

Artikel 4 Toegang tot en gebruik van ICT

4.1 @voCampus geeft de gebruiker het recht op toegang tot haar ICT en de daarmee verbonden systemen en faciliteiten, maar is te allen tijde bevoegd het recht op toegang weer in te trekken en toegang te onthouden.
4.2 Gebruikersidentificatie en authenticatie vindt plaats op gebruikersnaam en wachtwoord die door de ICT-dienst worden verstrekt. De gebruikersnaam en het wachtwoord zijn persoonsgebonden. Het is de gebruiker niet toegestaan om deze aan derden in gebruik te geven of met derden te delen. De gebruiker dient steeds zorgvuldig om te gaan met de gebruikersnaam en het wachtwoord, zodanig dat wordt voorkomen dat derden kennis daarvan kunnen nemen.
4.3 Voor applicaties waarbinnen met persoonsgegevens wordt gewerkt, is twee-factor-authenticatie verplicht.
4.4 Indien middels andere dan door @voCampus ter beschikking gestelde apparatuur toegang tot het gebruik van ICT van @voCampus wordt verkregen, is het niet toegestaan om schoolrelevante data en persoonsgegevens van anderen lokaal op te slaan of om bestandssynchronisatie toe te passen. Het is de gebruiker niet toegestaan om voor het opslaan van schooldata eigen opslagmedia (bijvoorbeeld: een USB-stick) te gebruiken.
4.5 Wanneer schoolmail op andere dan door @voCampus ter beschikking gestelde apparatuur wordt ontvangen, dient deze apparatuur afdoende beveiligd te zijn (bijvoorbeeld met behulp van een pincode of een vingerafdruk). Indien dit niet mogelijk is, dan mag uitsluitend de webmail gebruikt worden om toegang te krijgen tot de schoolmail.
4.6 Het is voor medewerkers niet toegestaan om ICT-apparatuur waarop men als gebruiker is aangemeld, in onbeheerde toestand achter te laten. (‘Locken’ met Windows-toets + L is afdoende.)

Artikel 5 Algemene regels ten aanzien van het gebruik van ICT

5.1 Het gebruik van ICT is primair verbonden met taken en bezigheden die voortvloeien uit het verzorgen of ontvangen van onderwijs en/of het begeleiden en/of het ondersteunen daarvan. Als uitgangspunt geldt dat het gebruik van ICT ten dienste moet staan aan het onderwijs.

5.2 Het gebruik van ICT dient steeds op een zodanige wijze plaats te vinden dat de integriteit van de ICT en de beveiliging daarvan niet kunnen worden aangetast.

5.3 Het gebruik van ICT dient steeds plaats te vinden naar de letter en de geest van de Gedragscode en het Privacyreglement.

5.4 Het is in het bijzonder niet toegestaan om:

- pornografisch, racistisch, discriminerend, seksueel intimiderend, beledigend of aanstootgevend materiaal te bekijken of te downloaden of te verspreiden;
- op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende manier via ICT te communiceren;
- computervirussen en andere software die de integriteit van de gegevens of de computerbeveiliging van ICT kunnen beschadigen, te introduceren of te verspreiden;
- ICT te gebruiken ten behoeve van strafbare gedragingen.

5.5 Het is niet toegestaan om foto's, video's of ander materiaal van op school werkzame personen of leerlingen of andere bij de school betrokkenen via ICT (daaronder ook begrepen: social media) te publiceren, tenzij dit gericht is op een aan de school gerelateerde doelstelling en de afgebeelde personen hebben aangegeven in te stemmen met dergelijke publicaties.

5.6 Indien en voor zover sprake is van het verwerken van persoonsgegevens, gebeurt dit met inachtneming van het Privacyreglement en de daarin opgenomen verwijzingen, zoals die met betrekking tot een verwerkersovereenkomst.

5.7 Het gebruik van eigen opslagmedia (bijvoorbeeld: een USB-stick) voor schooldata is niet toegestaan.

5.8 Een vermoeden van misbruik van ICT en inbreuken op de beveiliging, dienen steeds direct aan de direct leidinggevende en aan de ICT-dienst gemeld te worden, ongeacht of deze al dan niet bij toeval worden ontdekt conform het protocol 'datalek' (zie bijlage).

5.9 Als de gebruiker er niet zeker van is of een bepaald gebruik van ICT wel of niet verantwoord is, dan overlegt hij daarover met de ICT-dienst.

Artikel 6 Toegang tot en gebruik van internet en e-mail

6.1 Het bestuur van @voCampus is bevoegd om de toegang tot bepaalde sites door middel van een filtersysteem te beperken.

6.2 Ten aanzien van het versturen van e-mailberichten dient de gebruiker terughoudend om te gaan met persoonsgegevens en vertrouwelijke of anderszins gevoelige informatie.

6.3 Voor het verzenden en ontvangen van e-mailberichten waarbinnen schooldata aanwezig zijn, mag alleen gebruik gemaakt worden van mailfaciliteiten, zoals Outlook, Magister e.d., die @voCampus hiervoor beschikbaar stelt.

6.4 Voor het verzenden van e-mailberichten naar meerdere adressen buiten de school, dient voor adressering van het mailbericht altijd gebruik te worden gemaakt van het 'BCC-veld'.
6.5 Voor het verzenden van e-mailberichten naar adressen buiten de school, dient altijd gebruik te worden gemaakt van de optie 'beveiligde mail' indien de mail persoonsgegevens bevat.
6.6 Het is voor medewerkers niet toegestaan om schoolmail (automatisch) door te sturen naar privé-mail.
6.7 Om de integriteit van data en de continuïteit van werkzaamheden binnen @voCampus te kunnen waarborgen, mag voor opslag en verwerking van data uitsluitend gebruik gemaakt worden van door @voCampus beschikbaar gestelde en beheerde ICT-platforms. Programma's zoals het Google-platform, Gmail, Hotmail, Dropbox en WeTransfer zijn hiervoor dus niet geëigend.

Artikel 7 Specifieke regels voor contact middels ICT

7.1 Conform de Gedragscode en het Privacyreglement is privé-contact tussen medewerkers en leerlingen, binnen dan wel buiten schooltijd, door middel van e-mail, Whatsapp, MS Teams en andere social media in beginsel verboden.
7.2 Digitaal contact tussen leidinggevende en medewerker met betrekking tot formele, werk-gerelateerde zaken met daarin persoonsgegevens, dient via door @voCampus verstrekte mail- en online vergadermogelijkheden (MS Teams) plaats te vinden en niet via social media. Berichtendiensten zoals SMS, WhatsApp, Telegram en Signal worden derhalve uitsluitend gebruikt voor informele en meer vluchtige communicatie en dienen als zodanig geen persoonsgegevens of formele communicatie te bevatten.
7.3 Onderling digitaal contact tussen medewerkers over een leerling is uitsluitend toegestaan in verband met onderwijs-gerelateerde zaken en dient uitsluitend te verlopen via de schoolmail en MS Teams.

Artikel 8 Regels ten aanzien van het gebruik van social media

8.1 Indien social media voor onderwijs-, werkgerelateerde doeleinden worden gebruikt dient dit – met het oog op de bescherming van persoonsgegevens – steeds plaats te vinden conform de Gedragscode, het Privacyreglement en de AVG.
8.2 Gebruik van social media waarmee geen onderwijs- of werk gerelateerd doel wordt gediend, dient zoveel mogelijk buiten schooltijd plaats te vinden.
8.3 De gebruiker zal zich op social media niet uitlaten op een wijze die als smadelijk of lasterlijk beoordeeld kan worden, of die schadelijk kan zijn voor @voCampus, de scholen, personeelsleden, leerlingen en/of anderszins bij @voCampus betrokkenen, dit zoals ook bepaald in de Gedragscode en het Privacyreglement.
8.4 De gebruiker deelt op social media geen bedrijfsvertrouwelijke informatie van of over de school.
8.5 De gebruiker deelt op social media geen persoonsgegevens van personeelsleden, leerlingen en/of anderszins bij @voCampus betrokkenen waartoe hij uit hoofde van zijn functie en/of positie toegang heeft.

8.6 De gebruiker plaatst op social media niet zonder toestemming foto's of andere afbeeldingen van de school en/of aan de school verbonden personen.
8.7 De gebruiker plaatst op social media geen content namens (de scholen van) @voCampus, tenzij hij daarvoor toestemming heeft gekregen.

Artikel 9 Regels ten aanzien van controle op gebruik

9.1 Het is in het belang van @voCampus, de scholen, personeelsleden, leerlingen en/of anderszins bij @voCampus betrokkenen, dat er controle kan plaatsvinden op het gebruik van ICT. Het bevoegd gezag is bevoegd deze controle in te zetten wanneer daar zwaarwegende redenen voor zijn. Die controle zal plaatsvinden overeenkomstig de geldende wet- en regelgeving, waarbij steeds oog wordt gehouden voor de balans tussen verantwoord gebruik van ICT enerzijds en de bescherming van de privacy van de gebruikers anderzijds.
9.2 Het bestuur en de schoolleiding treffen voorzieningen voor de positie en de integriteit van de ICT-dienst en de ICT-medewerkers. De medewerkers van de ICT-dienst hebben een geheimhoudingsplicht die inhoudt dat ten aanzien van de verzamelde en voor hen inzichtelijke informatie strikte geheimhouding in acht genomen zal worden.
9.3 Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen. Indien een gebruiker of groep gebruikers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde periode, in opdracht van het bevoegd gezag, gerichte controle plaatsvinden.
9.4 Controle van persoonsgegevens met betrekking tot gebruik van ICT vindt slechts plaats in het kader van handhaving van de doelen van dit protocol.
9.5 Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik, inclusief social mediagebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van het bevoegd gezag, controle op inhoud plaats.
9.6 Verboden e-mail- en internetgebruik worden zo veel mogelijk softwarematig onmogelijk gemaakt.
9.7 Controle van persoonsgegevens met betrekking tot gebruik van ICT vindt slechts plaats in het kader van handhaving van de doelen van dit protocol.
9.8 E-mailberichten van leden van een medezeggenschapsorgaan onderling, van vertrouwenspersonen, van bedrijfsartsen en van eenieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in beginsel niet gecontroleerd. Dit geldt niet voor de veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.

Artikel 10 Regels ten aanzien van de uitvoering van de controle

10.1 De controle op persoonsgegevens bij gebruik van ICT vindt slechts plaats met als doel:
- het tegengaan van onverantwoord en ontoelaatbaar gebruik;
- de naleving van dit protocol, de Gedragscode en het Privacyreglement;
- het bewaken van de voortgang van werkzaamheden (bij langdurige afwezigheid of beëindiging van het dienstverband van een medewerker);
- het vastleggen van bewijs en/of archief;

- de systeem- en netwerkbeveiliging;
- de kosten- en capaciteitsbeheersing.

10.2 Bij ernstige verdenking van gebruik van ICT in strijd met dit protocol en/of bezit van ongeoorloofde data, is het bestuur van @voCampus bevoegd om gedurende het nader onderzoek dienaangaande, het account van de betreffende gebruiker te blokkeren en/of de aan de betreffende gebruiker ter beschikking gestelde ICT-apparatuur in beslag te nemen.

10.3 In het kader van de controle op de gebruikers voor het doel als bedoeld in artikel 10.1, geldt dat indien er een concreet vermoeden is dat een gebruiker de regels, waarvan de naleving wordt gecontroleerd, overtreedt, er zo nodig een in tijd en omvang zo beperkt mogelijke gerichte controle op persoonsniveau plaatsvindt.

10.4 De controle op gebruik van ICT zal, overeenkomstig dit protocol, in beginsel uitgevoerd worden door alleen medewerkers van de ICT-dienst en uitsluitend in opdracht van het bevoegd gezag.

Artikel 11 Disciplinaire maatregelen

11.1 Indien wordt vastgesteld dat een medewerker gebruik heeft gemaakt van ICT op een wijze die strijdig is met dit protocol, is het bestuur dan wel de schoolleiding bevoegd de medewerker tijdelijk uit te sluiten van inlogmogelijkheden en jegens hem een (disciplinaire en/of rechtspositionele) maatregel te treffen. Bij het bepalen van de maatregel wordt rekening gehouden met de aard en ernst van de wijze waarop in strijd met dit protocol gebruik is gemaakt van ICT.

11.2 Indien wordt vastgesteld dat een leerling gebruik heeft gemaakt van ICT op een wijze die strijdig is met dit protocol, kan de schoolleiding, afhankelijk van de aard en de ernst van het onverantwoorde gebruik, overgaan tot het tijdelijk uitsluiten van inlogmogelijkheden voor de betrokken leerling, het melden van dit gedrag en de consequenties daarvan aan de ouder(s)/verzorger(s) en/of het opleggen van een (straf)maatregel, waaronder schorsing en/of verwijdering.

Artikel 12 Klachten

12.1 Wanneer een betrokkene van mening is dat het doen of nalaten door het bevoegd gezag van @voCampus niet in overeenstemming is met dit protocol, met de AVG, of (andere) toepasselijke wet- of regelgeving, dan kan een klacht worden ingediend overeenkomstig de binnen @voCampus geldende klachtenregeling. Een betrokkene kan zich eveneens wenden tot de functionaris gegevensbescherming van @voCampus voor AVG-gerelateerde zaken.

Artikel 13 Overige bepalingen

13.1 Als zich situaties voordoen waarin dit protocol niet voorziet, dan zal conform de letter en de geest van dit protocol, de gedragscode, het privacyreglement dan wel de AVG gehandeld worden.

13.2 Als de situatie zich voordoet waarin sprake is van een datalek, dient conform de letter en de geest van dit protocol en het protocol 'datalek' gehandeld te worden. Protocol datalek is toegevoegd als bijlage.
13.3 De functionaris gegevensbescherming rapporteert jaarlijks aan het Bestuur over de naleving van dit Protocol.
13.4 Jaarlijks wordt door het Bestuur gerapporteerd aan de (G)MR over de naleving van het Protocol, waarin ook het aantal incidenten vermeld wordt.
13.5 Dit protocol ICT en social media is ter instemming voorgelegd aan de GMR.
13.6 Dit protocol treedt in werking per 1 januari 2022 en wordt op de website van @voCampus gepubliceerd.
13.7 Dit protocol wordt binnen twee jaar na inwerkingtreding geëvalueerd.

Bijlage 1

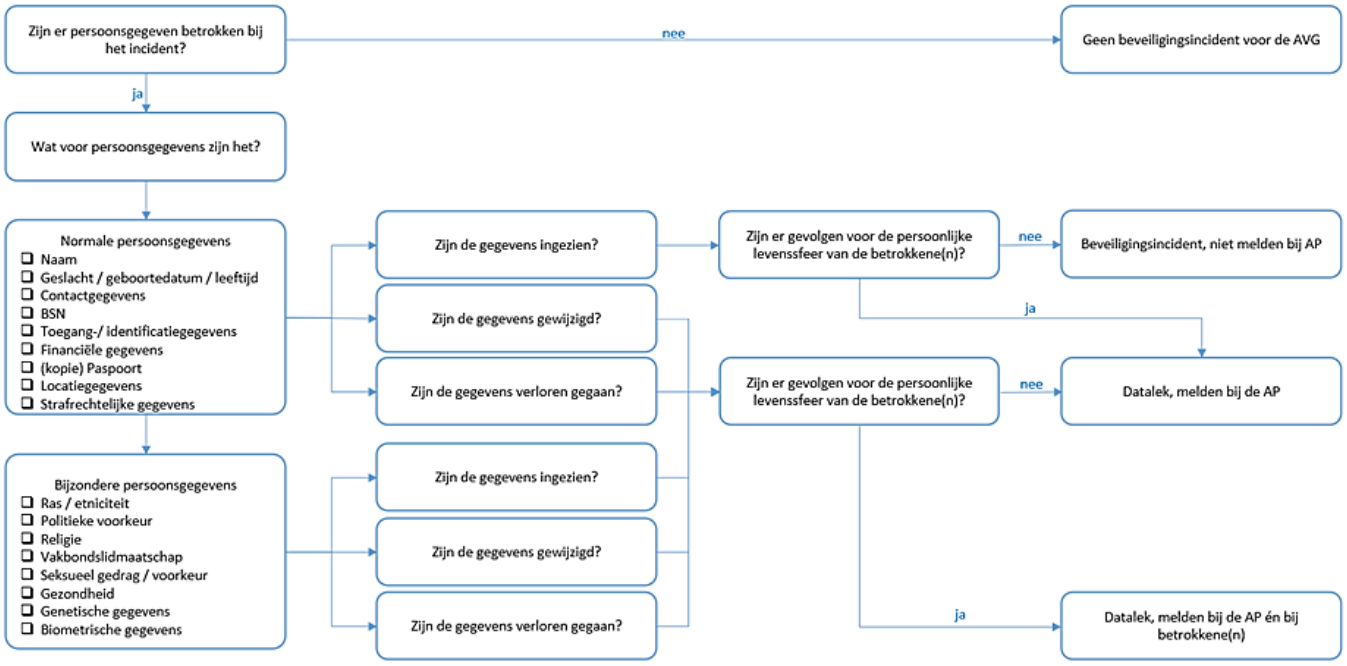
Datalekprotocol

De AVG geeft in artikel 4 de volgende definitie van een inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Vrij vertaald betekent dit dat als er sprake is van het verkrijgen van toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie, of zonder dat dit wettelijk is toegestaan, sprake is van een beveiligingsincident, dan wel datalek. Dit kan zowel opzettelijk als onopzettelijk gebeuren.

Er zit een verschil in gradatie tussen een beveiligingsincident en een datalek. Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar is of kan komen. Een datalek is een beveiligingsincident, waarbij persoonsgegevens verloren raken of onrechtmatig worden verwerkt (opgeslagen, aangepast, verzonden, enz.). Alle datalekken zijn dus beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken. Datalekken moeten binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens (AP), terwijl beveiligingsincidenten alleen opgenomen hoeven te worden in het interne register van incidenten.

Om te bepalen of een beveiligingsincident een datalek is, is onderstaand stroomschema ontwikkeld. Naast de meldplicht voor datalekken is er ook de verplichting om alle beveiligingsincidenten registreren. Dat geldt óók voor alle incidenten die niet gemeld hoeven te worden aan de AP. Deze kan altijd om inzage hiervan vragen.



Een beveiligingsincident of datalek meld je zo spoedig mogelijk bij je direct leidinggevende en de privacyverantwoordelijke op school en Functionaris Gegevensbescherming (FG) via m.schoonus@vocampus.nl of 06 – 13 68 32 83.

Stappenplan datalekken

Stap 1 Zorg voor overzicht

Analyseer de situatie. Zorg dat je weet wat er is gebeurd en wat de omvang van het lek is. Gaat het om een inbreuk op de privacy door gelekte, vernietigde of gewijzigde gegevens? Wie heeft er mogelijk toegang (gehad) tot welke persoonsgegevens? Deze informatie wordt vastgelegd met daarin in ieder geval:

- Datum / periode van het beveiligingsincident
- Aard van het beveiligingsincident
- Omschrijving van de groep betrokkenen
- Aantal betrokkenen
- Type persoonsgegevens in kwestie
- Worden de gegevens binnen de keten gedeeld?

Stap 2 Beperk de schade

Op basis van de uitkomst van de gegevensverzameling in stap 1 wordt bepaalt of en zo ja welke maatregelen direct getroffen moeten worden. Om het lek te beëindigen en de schade te beperken. Schakel hiervoor zo nodig de juiste hulp in, bijvoorbeeld van de ICT-dienst.

Stap 3 Meld het datalek
De functionaris gegevensbescherming maakt de afweging of een datalek gemeld dient te worden bij de Autoriteit Persoonsgegevens (AP). Deze melding dient binnen 72 uur na ontdekking van het datalek plaats te vinden. In sommige gevallen moet een datalek ook aan betrokken personen gemeld worden. Dit is het geval als er sprake is van een verhoogd risico voor de rechten en vrijheden van betrokken personen.

Stap 4 Registreer
Tenslotte registreert de FG het datalek of beveiligingsincident in het datalekregister. Dit is een register, waar alle incidenten in worden bijgehouden en wat zo nodig ter beschikking van de AP gesteld moet worden. Het register dient ook als handvat om te kijken wat voor datalekken voorkomen, zodat training op dit onderdeel mogelijk wordt.

Belangrijk om te weten
Een datalek melden is niet erg. Het geeft aan dat je je bewust bent van de regels rondom privacy op school en een juiste inschatting gemaakt hebt wat betreft de mogelijke gevolgen van een datalek. Een tijdig gemeld datalek vormt ook een verkleining van het risico voor de organisatie. Je zult er dan ook nooit persoonlijk op worden afgerekend.

Een bewust niet gemeld datalek vormt juist een groot risico voor de organisatie en zal als het via een andere weg bij de AP terecht komt, vaak leiden tot een onderzoek met een mogelijke geldboete en imageschade als gevolg.