Privacyreglement leerlingen

SOOOG

Stichting Openbaar Onderwijs
Oost Groningen

Inhoud

Inleiding

Dit document is niet van toepassing op personeelsgegevens.

Voor algemene informatie over de verwerking van persoonsgegevens verwijzen we onder andere naar de website van de Autoriteit Persoonsgegevens en naar het ministerie van Justitie. Voor de tekst van de Wet bescherming persoonsgegevens en de tekst van het Vrijstellingsbesluit Wet bescherming persoonsgegevens verwijzen we naar de website www.wetten.overheid.nl.

Met dit privacyreglement wil Stichting Openbaar Onderwijs Oost Groningen duidelijkheid geven over het beleid en de regels van de organisatie rondom de omgang met privacy en persoonsgegevens.

1. Definities

In dit privacyreglement wordt verstaan onder:

Persoonsgegevens
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

> *Uitleg: alle gegevens die informatie geven over een bepaald iemand zijn persoonsgegevens in de zin van de wet. Denk hierbij aan naam, adresgegevens, Burgerservicenummer, maar ook aan foto's of een leerling-nummer.*

Verwerking van persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

> *Uitleg: verwerken betekent alles wat er met die gegevens gebeurt, zoals veranderen, verwijderen of toegang geven aan iemand anders.*

Bijzonder persoonsgegeven
Een persoonsgegeven dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid of zijn gezondheid.

Wettelijk vertegenwoordiger
Indien een leerling de leeftijd van zestien jaren nog niet heeft bereikt, wordt de leerling vertegenwoordigd door zijn wettelijk vertegenwoordiger. Meestal zal dit een ouder zijn, maar het kan hier ook gaan om een voogd.

> *Uitleg: als je nog geen 16 jaar bent, mag alleen jouw wettelijk vertegenwoordiger (denk aan jouw ouders of voogd) bijvoorbeeld toestemming geven aan de school om*

foto's van jou te mogen plaatsen op de schoolwebsite. Als je ouder bent dan 16, mag je deze beslissingen zelf nemen.

Verantwoordelijke
De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Wanneer er in dit reglement gesproken wordt over de verantwoordelijke dan wordt daarmee Stichting Openbaar Onderwijs Oost Groningen bedoeld.

Bewerker
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Uitleg: de bewerker is degene die in opdracht van Stichting Openbaar Onderwijs Oost Groningen persoonsgegevens verwerkt. Dat kan ook buiten de organisatie van de school zijn.

Datalek
Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker.
Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten.
Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens.

Wpb
Wet bescherming persoonsgegevens.

2. De reikwijdte en het doel van dit reglement

1. Dit reglement stelt regels vast over de verwerking van persoonsgegevens van leerlingen en hun wettelijke vertegenwoordiger door Stichting Openbaar Onderwijs Oost Groningen.
2. Dit reglement is van toepassing op alle persoonsgegevens van leerlingen en hun wettelijk vertegenwoordiger die door Stichting Openbaar Onderwijs Oost Groningen worden verwerkt. Het doel van dit reglement is:
    a. Vaststellen welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt.
    b. De privacy van de leerling en zijn/haar wettelijk vertegenwoordiger beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens.
    c. De zorgvuldige verwerking van persoonsgegevens borgen.
    d. De rechten van leerling en zijn/haar wettelijk vertegenwoordiger beschermen.

3. Het doel van de verwerking van persoonsgegevens

1. Bij de verwerking van persoonsgegevens houdt Stichting Openbaar Onderwijs Oost Groningen zich aan de wet, waaronder de Wet bescherming persoonsgegevens. De verwerking van persoonsgegevens doet Stichting Openbaar Onderwijs Oost Groningen uitsluitend voor:
    a. Het geven van het onderwijs, het begeleiden en ondersteunen van leerlingen en het geven van studieadviezen.
    b. Het verstrekken of ter beschikking stellen van leermiddelen.
    c. Het bekend maken van informatie over Stichting Openbaar Onderwijs Oost Groningen en haar leerlingen, bijvoorbeeld op de website van Stichting Openbaar Onderwijs Oost Groningen.
    d. Het bekendmaken van de activiteiten van Stichting Openbaar Onderwijs Oost Groningen, bijvoorbeeld op de website van Stichting Openbaar Onderwijs Oost Groningen.
    e. Het berekenen, vastleggen en innen van inschrijvingsgelden, lesgelden, bijdragen of vergoedingen voor leermiddelen en activiteiten, waaronder begrepen het eventueel uit handen geven van dergelijke vorderingen aan derden.
    f. Het behandelen van geschillen en het doen uitoefenen van accountantscontrole.
    g. Het contact houden met oud-leerlingen van Stichting Openbaar Onderwijs Oost Groningen.
    h. De uitvoering of toepassing van een wettelijke verplichting van Stichting Openbaar Onderwijs Oost Groningen.
2. Stichting Openbaar Onderwijs Oost Groningen verwerkt niet meer gegevens dan noodzakelijk is om de hiervoor beschreven doelen te bereiken.

4. Vrijstelling

1. De in artikel 3 genoemde gegevensverwerkingen vallen onder het vrijstellingsbesluit Wet bescherming persoonsgegevens. Dit houdt in dat Stichting Openbaar Onderwijs Oost Groningen niet bij de Autoriteit Persoonsgegevens hoeft te melden dat zij persoonsgegevens verwerkt. Uiteraard blijft Stichting Openbaar Onderwijs Oost Groningen onder toezicht van de Autoriteit Persoonsgegevens opereren.

5. De soorten gegevens die verwerkt worden

1. De persoonsgegevens worden verwerkt voor de volgende categorieën met omschrijving:
    a. Naam, voornamen, voorletters, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de leerling.
    b. Het Burgerservicenummer (BSN) van de leerling.
    c. Nationaliteit van de leerling.

d. Naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de wettelijk vertegenwoordiger(s) van de leerling.
e. Gegevens over de gezondheid of het welzijn van de leerling die noodzakelijk zijn voor ondersteuning van de betreffende leerling.
f. Gegevens over de godsdienst of levensovertuiging van de leerling die noodzakelijk zijn voor de school, het onderwijs of de te geven ondersteuning.
g. Gegevens over de aard en het verloop van het onderwijs en ondersteuning, en de behaalde leerresultaten.
h. Schoolgegevens (waaronder naam school, naam zorgcoördinator/mentor/intern begeleider, klas/groep waar de leerling in zit, tijdstip van inschrijving bij deze school, schoolloopbaan en rapportage vanuit primair en voortgezet onderwijs).
i. Eventuele aanleiding voor de aanmelding bij het samenwerkingsverband passend onderwijs, relevante screenings- en onderzoeksgegevens en omschrijving van de problematiek die aan de orde is.
j. Activiteiten die door de school zijn ondernomen rond de leerling, en ook de resultaten hiervan.
k. Bestaande of (relevante) afgesloten hulpverleningscontacten en de namen van contactpersonen.
l. Relevante persoonsgegevens die door externe partijen worden verstrekt over de aangemelde problematiek van de leerling.
m. Relevante financiële gegevens over bijvoorbeeld (vrijwillige) financiële bijdragen.

6. Het beheer van (de verwerking van) persoonsgegevens

1. Persoonsgegevens worden op naam van de leerling verzameld. De verzameling van persoonsgegevens van de leerling vormt het dossier.

7. De grondslag voor de verwerking

1. Verwerking van persoonsgegevens gebeurt alleen op grond van:
    a. Toestemming: als de leerling en zijn/haar wettelijk vertegenwoordiger voor de verwerking zijn toestemming heeft verleend. Voor het gebruik van foto's en video's door Stichting Openbaar Onderwijs Oost Groningen zal bijvoorbeeld apart toestemming gevraagd worden via een toestemmingsbrief.
    b. Overeenkomst: als de gegevensverwerking noodzakelijk is voor het sluiten of de uitvoering van een overeenkomst waarbij de leerling en zijn/haar wettelijk vertegenwoordiger partij is, denk hierbij aan een schoolinschrijving of –uitschrijving.
    c. Wettelijke verplichting: als de gegevensverwerking noodzakelijk is op grond van een wet waaraan Stichting Openbaar Onderwijs Oost Groningen zich moet houden.
    d. Vitaal belang: als de leerling en zijn/haar wettelijk vertegenwoordiger een vitaal belang heeft bij de gegevensverwerking, denk hierbij aan het melden

van een allergie op het moment dat een leerling iets heeft gegeten waarvoor hij/zij allergisch is.

e. Gerechtvaardigd belang: als Stichting Openbaar Onderwijs Oost Groningen een gerechtvaardigd belang heeft om de persoonsgegevens te verwerken, tenzij het recht op privacy van de leerling en zijn/haar wettelijk vertegenwoordiger hierboven gaat.

8. Monitoren van ICT en internetgebruik op school

1. Voor het gebruik van ICT-systemen en internet op school wordt gebruik gemaakt van software waarmee ICT en internetgebruik door leerlingen gecontroleerd kan worden.
2. Stichting Openbaar Onderwijs Oost Groningen slaat gegevens over het gebruik van ICT en internet door leerlingen op voor de volgende doelen:
    a. Het beschermen van leerlingen tegen blootstelling aan ongewenste sociale media en websites (vulgaire websites kunnen bijvoorbeeld met behulp van die data worden geblokkeerd).
    b. Het verbeteren van de ICT-systemen.
    c. Het opsporen van leerlingen die schade aan de ICT-systemen hebben veroorzaakt.
    d. Het blokkeren van usb-poorten, bepaalde software en sociale media wanneer dit ongewenst is (bijvoorbeeld in bepaalde lessen).

9. Bewaartermijnen

1. Stichting Openbaar Onderwijs Oost Groningen bewaart de persoonsgegevens niet langer dan noodzakelijk is voor het vervullen van het doel waarvoor zij zijn verkregen.
2. De persoonsgegevens worden in ieder geval verwijderd uiterlijk twee jaren nadat de studie is beëindigd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.

10. De doorgifte van persoonsgegevens aan derden

1. De school verleent slechts toegang tot in de administratie en systemen van de school opgenomen persoonsgegevens aan:
    a. Een bewerker die Stichting Openbaar Onderwijs Oost Groningen inschakelt voor het bereiken van de doelen die worden genoemd in artikel 3, denk hierbij aan een bedrijf dat het voor de leerling of wettelijk vertegenwoordiger mogelijk maakt om online de rapportcijfers van een leerling in te zien.
    b. Derden die op grond van de wet toegang moet worden verleend, waarbij alleen toegang wordt verleend tot de gegevens waartoe volgens de wet toegang moet worden gegeven.

11. De rechten van leerlingen en de wettelijk vertegenwoordiger

1. De wettelijk vertegenwoordiger en de leerling die 16 jaar of ouder is kan bij Stichting Openbaar Onderwijs Oost Groningen verzoeken om een volledig overzicht van zijn/haar verwerkte persoonsgegevens. Het verzoek wordt binnen vier weken beantwoord (zie artikel 35, Wet bescherming persoonsgegevens). De kosten van dit verzoek zijn maximaal 5 euro.
2. De wettelijk vertegenwoordiger en de leerling die 16 jaar of ouder is kan verzoeken zijn/haar persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Denk hierbij aan het verbeteren van een verkeerd gespelde naam of het doorgeven van een verhuizing. Dit verzoek is alleen mogelijk als deze persoonsgegevens niet (meer) kloppen, niet nodig zijn of niet mogen worden verwerkt volgens de wet. Het verzoek wordt binnen vier weken beantwoord (zie artikel 36, Wet bescherming persoonsgegevens).
3. De wettelijk vertegenwoordiger en de leerling die 16 jaar of ouder is kan bij Stichting Openbaar Onderwijs Oost Groningen verzet aantekenen tegen de verwerking van zijn/haar persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. Stichting Openbaar Onderwijs Oost Groningen oordeelt binnen vier weken na ontvangst van het verzet of dit gerechtvaardigd is. Als Stichting Openbaar Onderwijs Oost Groningen het verzet gerechtvaardigd acht, beëindigt Stichting Openbaar Onderwijs Oost Groningen meteen de verwerking (zie artikel 40, Wet bescherming persoonsgegevens).

12. Beveiliging en geheimhouding van persoonsgegevens

1. Stichting Openbaar Onderwijs Oost Groningen zal ervoor zorgen dat de persoonsgegevens beveiligd worden met passende technische en organisatorische maatregelen, om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt door anderen. Deze maatregelen voorkomen ook onnodige verzameling of verwerking van persoonsgegevens.
2. Stichting Openbaar Onderwijs Oost Groningen zal ervoor zorgen dat medewerkers van de school niet meer inzage of toegang hebben tot de persoonsgegevens dan noodzakelijk is voor een goede uitoefening van hun werk.
3. Stichting Openbaar Onderwijs Oost Groningen zal ervoor zorgen dat persoonsgegevens, die vertrouwelijk zijn of geheim moeten worden gehouden (zoals bijvoorbeeld bijzondere persoonsgegevens over de gezondheid van een leerling), ook geheim worden gehouden door de medewerkers van Stichting Openbaar Onderwijs Oost Groningen.

13. Het melden van datalekken

1. Melden aan de Autoriteit Persoonsgegevens

Niet ieder datalek hoeft worden gemeld aan de Autoriteit Persoonsgegevens. Volgens de wet moet men een melding doen aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Bij persoonsgegevens van gevoelige aard denken we aan:

- *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp.* Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, geaarelidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- *Gegevens over de financiële of economische situatie van de betrokkene.* Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene.* Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- *Gebruikersnamen, wachtwoorden en andere inloggegevens.* De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude.* Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (BSN).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het mogelijk dat een datalek moet worden gemeld waar de persoonsgegevens van slechts één persoon bij betrokken zijn.

Melding dient te worden gedaan zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar. Via dit webformulier kunnen meldingen zo nodig worden aangevuld of worden ingetrokken.

2. Melden aan de betrokkene

Als tot de conclusie wordt gekomen dat een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens, dan betekent dit niet automatisch dat dit datalek ook moet worden gemeld aan de betrokkene (de wettelijk vertegenwoordiger of een leerling die 16 jaar of ouder is). Hiervoor dient een aparte afweging te worden gemaakt.

- De wet geeft aan dat een melding moet worden gedaan aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Hierbij valt te denken aan onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan kan men er in principe van uit gaan dat men het datalek niet alleen moet melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene.

- De melding stelt de betrokkene in staat om alert te zijn op de mogelijke gevolgen van het datalek en om zich daar waar mogelijk tegen te wapenen door, bijvoorbeeld, een gelekt wachtwoord te vervangen. De wet schrijft voor dat de melding *onverwijld* moet worden gedaan. Daarbij moet men rekening houden met het feit dat de betrokkene naar aanleiding van de melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene daarover wordt geïnformeerd, hoe eerder deze in actie kan komen.

- Als er passende technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene achterwege worden gelaten. Bij deze beschermingsmaatregelen moet men bijvoorbeeld denken aan cryptografische bewerkingen zoals encryptie en hashing. Men moet per geval bepalen of de maatregelen die zijn genomen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten.

3. Melding aan het College van Bestuur

Zodra er sprake is van het vermoeden dat er zich een datalek heeft voorgedaan wordt het College van Bestuur altijd *onverwijld* van dit vermoeden op de hoogte gebracht. Deze melding dient zowel telefonisch als schriftelijk, middels "Het Protocol melding datalekken" te worden gedaan. Dit Protocol is als bijlage 1 toegevoegd aan dit document en is tevens beschikbaar via de website van SOOOG (www.sooog.nl).

4. Uitzondering op de meldplicht

De meldplicht datalekken uit de Wbp is niet van toepassing als de Wbp niet van toepassing is. Dit is bijvoorbeeld het geval als men uitsluitend voor persoonlijke of huishoudelijke doeleinden persoonsgegevens verwerkt.

- De melding hoeft ook niet door Stichting Openbaar Onderwijs Oost Groningen te

worden gedaan als er zwaarwegende redenen zijn om geen melding aan de wettelijk vertegenwoordiger en de leerling die 16 jaar of ouder is te doen. Denk hierbij aan vertrouwelijke meldingen die een leerling heeft gedaan over zijn thuissituatie. Een inbreuk op de beveiliging van dergelijke gegevens zal niet gemeld worden aan de wettelijk vertegenwoordiger.

14. Klachten

1. Klachten over de inhoud van dit reglement kunnen gemeld worden aan Stichting Openbaar Onderwijs Oost Groningen en wel op het volgende e-mailadres: info@sooog.nl. Deze klacht wordt binnen vier weken vertrouwelijk behandeld.

15. Transparantie

1. Stichting Openbaar Onderwijs Oost Groningen informeert de betrokkene of diens wettelijk vertegenwoordiger over de verwerking van zijn persoonsgegevens. Indien het type verwerking dat vraagt, informeert Stichting Openbaar Onderwijs Oost Groningen iedere betrokkene apart over de details van die verwerking.
2. Stichting Openbaar Onderwijs Oost Groningen informeert de betrokkene of diens wettelijk vertegenwoordiger – op hoofdlijnen – ook over de afspraken die gemaakt zijn met derden en bewerkers die persoonsgegevens van de betrokkene ontvangen.

16. Slotbepaling

1. De Gemeenschappelijke Medezeggenschapsraad van Stichting Openbaar Onderwijs Oost Groningen heeft haar instemming gegeven voor de inhoud van dit document.
2. In het geval van onvoorziene omstandigheden, is Stichting Openbaar Onderwijs Oost Groningen gerechtigd van dit reglement af te wijken, een en ander slechts indien er sprake is van een direct en zwaarwegend belang voor Stichting Openbaar Onderwijs Oost Groningen of de leerling en de wettelijk vertegenwoordiger.
3. Stichting Openbaar Onderwijs Oost Groningen en haar Gemeenschappelijke Medezeggenschapsraad kunnen dit reglement in onderling overleg wijzigen of aanpassen. Aanpassingen of wijzigingen worden schriftelijk vastgelegd en door Stichting Openbaar Onderwijs Oost Groningen en haar Gemeenschappelijke Medezeggenschapsraad ondertekend. Vervolgens zal de wijziging bekend worden gemaakt aan de leerling en de wettelijk vertegenwoordiger.

17. Inwerkingtreding en duur

1. Dit reglement kan aangehaald worden als "Privacyreglement leerlingen" en treedt in werking op ##DATUM##.
2. Dit reglement zal, na inwerkingtreding, iedere twee jaar worden herzien en opnieuw goedgekeurd moeten worden.
3. SOOOG is bevoegd om evidente verschrijvingen in het reglement te corrigeren, dan wel tekstuele aanpassingen te doen, indien en voor zover dit de inhoud, aard en strekking van dit reglement en de daarin opgenomen bepalingen niet doen wijzigen.

Daadwerkelijke inhoudelijke wijzigingen in dit privacyreglement zullen, indien van toepassing, ter instemming worden voorgelegd aan Gemeenschappelijke Medezeggenschapsraad.

18. Registratie intern gebruik persoonsgegevens

Overzicht van diegenen die toegang hebben tot de persoonsgegevens van Stichting Openbaar Onderwijs Oost Groningen zoals bedoeld in dit reglement. We gebruiken hiervoor het document "Registratie intern gebruik persoonsgegevens". Dit document is als bijlage 2 toegevoegd.
Dit document dient voor al diegenen die toegang hebben tot persoonsgegevens te worden ingevuld. Het ondertekende document dient door de instelling te worden gearchiveerd.

19. Gebruik van dit privacyreglement

Gebruik van dit privacyreglement
Het geheel of gedeeltelijk gebruik van dit privacyreglement is uitsluitend toegestaan door de rechtmatige licentienemer van YourSafetynet school+. De inhoud van dit privacyreglement is beschermd door copyright © waardoor het niet is toegestaan om dit privacyreglement:

- Te vermenigvuldigen en/of openbaar te maken door middel van druk, fotokopie, microfilm of op enigerlei wijze zonder nadrukkelijke schriftelijke toestemming van Media Security Networks BV.
- Te gebruiken indien de huidige licentieovereenkomst van YourSafetynet school+ is vervallen.

Dit document is zorgvuldig en naar beste weten samengesteld. Regel- en wetgeving zijn voortdurend aan verandering onderhevig waardoor Media Security Networks BV niet kan instaan voor de juistheid of volledigheid hiervan. Media Security Networks BV aanvaardt geen enkele aansprakelijkheid voor schade, van welke aard dan ook, als gevolg van handelingen en/of beslissingen die op basis van dit privacyreglement zijn genomen.

Bijlage 1: Protocol melding datalekken

Van	**Stichting Openbaar Onderwijs Oost Groningen**
Aan	Verantwoordelijke en (veiligheids)functionaris
Betreft	Protocol melding datalekken
Document / Revisie	YSNS 33048 - Revisie 3.2

Melding datalekken

Let op! *Ernstige datalekken moeten binnen 72 uur na ontdekking gemeld te worden bij de Autoriteit Persoonsgegevens. Ga voor meer informatie naar:*
https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

Voorbeelden van ernstige datalekken:

- Inloggegevens, gebruiksnamen en wachtwoorden
- Financiële gegevens
- Kopieën van identiteitsbewijzen
- Werkprestaties
- Gegevens die betrekkingen hebben op levensovertuiging
- Gegevens die kunnen leiden tot stigmatisering of uitsluiting
- Gegevens die betrekking hebben op gezondheid
- Verlies USB stick, laptop of alternatieve datadragers met privacygevoelige informatie die naar personen kan leiden

Indien dit datalek waarschijnlijk ongunstige gevolgen heeft voor diens persoonlijke levenssfeer van de personen of organisaties van wie de gegevens gelekt zijn, dient – naast de melding naar de toezichthouder- het lek onverwijld gemeld te worden aan de personen of organisaties van wie de gegevens gelekt zijn. Ongunstige gevolgen zijn bijvoorbeeld identiteitsfraude, discriminatie en reputatieschade.

Via de website van SOOOG wordt een standaard formulier beschikbaar gesteld voor het melden van het datalek. Vervolgens wordt dit in het register van SOOOG opgeslagen, dat niet openbaar is. Indien er sprake is van een boete, dan zal deze melding openbaar gemaakt worden.

Moet een bewerker het datalek melden aan de Autoriteit Persoonsgegevens?

In veel gevallen wordt het verwerken van persoonsgegevens uitbesteed aan een derde partij. Deze derde partij noemt de wet een bewerker. Data kan bijvoorbeeld toegankelijk zijn voor een Cloud-dienstverlener die updates uitvoert op software, opgeslagen staan bij een hosting-provider, of beschikbaar zijn voor het marketing bedrijf dat e-mails in opdracht van klanten verzendt.

Een bewerker hoeft een datalek niet te melden bij de Autoriteit Persoonsgegevens. Wel moet de bewerker er voor zorgen dat haar opdrachtgever deze melding tijdig bij de Autoriteit Persoonsgegevens kan maken. Er zullen daarom schriftelijke afspraken moeten worden gemaakt waarin wordt vastgelegd op welke wijze de klanten door de bewerker op de hoogte worden gesteld van een datalek.

Wie is verantwoordelijk voor de uitvoering protocol melding datalekken?

Alleen de verantwoordelijke (of functionaris die namens verantwoordelijke is geautoriseerd) is bevoegd om namens Stichting Openbaar Onderwijs Oost Groningen uitvoering te geven aan het protocol melding datalekken.

	Uitvoerder protocol melding datalekken
Naam	Mw. Alida Meijering
Functie	Bestuurssecretaresse SOOOG
Datum **(later in te vullen)**	
Handtekening **(later in te vullen)**	

1. Analyse voordat tot het melden van een mogelijk datalek wordt overgegaan:

Vink JA of NEE aan.

Melden datalek	**JA**	**NEE**
Valt de verwerking onder de meldplicht?		
Is men krachtens het vrijwaringbesluit vrijgesteld om deze verwerking te melden? Ga voor een toelichting naar: Wizard uitvoering privacybeleid en selecteer vraag 8.		
Zijn er waarschijnlijk nadelige gevolgen voor privépersonen of organisaties?		
Zijn de betrokkenen schriftelijk over het datalek geïnformeerd?		
Hoe en wanneer het datalek* gemeld: *De melding kan achteraf worden gewijzigd, aangevuld dan wel worden ingetrokken.		

- Via het webformulier		
- Uiterlijk 2e werkdag na ontdekking van het incident		
- Via het webformulier		
Zijn er zwaarwegende argumenten het datalek niet te melden?		

2. Onderstaande gegevens <u>moeten</u> geregistreerd worden.

Registratie datalek gegevens	**Antwoord**
Datum en tijdstip ontdekking van het datalek?	
Wie heeft het datalek ontdekt?	
Wat is de oorzaak van het datalek?	
Welke privacy- of persoonsgevoelige gegevens zijn precies gelekt?	
Zijn de gelekte gegevens versleuteld (encryptie) waardoor de inhoud in principe onleesbaar is voor derden?	
Met welk argument(en) is het datalek niet gemeld?	
Wat zijn de aanbevolen maatregelen ter voorkoming van negatieve gevolgen?	
Wat zijn de vermoedelijke gevolgen van het datalek?	
Wat zijn de getroffen maatregelen ter voorkoming van de gevolgen?	
Op welke wijze is het lek gedicht?	
Wat is gedaan om herhaling te voorkomen?	

Wat is de communicatiestrategie zowel binnen als buiten de organisatie?	

Gebruik van dit protocol melding datalekken

Het geheel of gedeeltelijk gebruik van dit protocol melding datalekken is uitsluitend toegestaan door de rechtmatige licentienemer van YourSafetynet school+. De inhoud van dit protocol melding datalekken is beschermd door copyright © waardoor het niet is toegestaan om dit protocol melding datalekken:

- te vermenigvuldigen en/of openbaar te maken door middel van druk, fotokopie, microfilm of op enigerlei wijze zonder nadrukkelijke schriftelijke toestemming van Media Security Networks BV
- te gebruiken indien de huidige licentieovereenkomst van YourSafetynet school+ is vervallen

Deze procedure melding datalekken is zorgvuldig en naar beste weten samengesteld. Regel- en wetgeving zijn voortdurend aan verandering onderhevig waardoor Media Security Networks BV niet kan instaan voor de juistheid of volledigheid hiervan. Media Security Networks BV aanvaardt geen enkele aansprakelijkheid voor schade, van welke aard dan ook, als gevolg van handelingen en/of beslissingen die op basis van dit protocol melding datalekken zijn genomen.

Bijlage 2: Registratie intern gebruik persoonsgegevens

Van	Stichting Openbaar Onderwijs Oost Groningen
Aan	Alle leerkrachten en medewerkers
Betreft	Registratie intern gebruik persoonsgegevens
Document / Revisie	YSNS 33052 - Revisie 3.3.

Medewerker

	Medewerker
Datum	
Naam	
Functie	

Toegang tot privacygevoelige informatie of persoonsgegevens?

Vink JA of NEE aan, of vink '?' aan indien onbekend.

	?	JA	NEE
Heeft u op dit moment toegang tot privacygevoelige informatie of persoonsgegevens?			
Bent u specifiek geautoriseerd om toegang te krijgen tot deze gegevens?			
	Datum		
Sinds wanneer heeft u toegang tot deze gegevens (indien van toepassing)?	____ - ____ - _____		

Is uw antwoord op de eerste vraag 'NEE', dan kunt u de rest van dit formulier overslaan.

Tot welke (privacy)gevoelige gegevens heeft u op dit moment toegang?

Vink aan wat voor u van toepassing is; maak een keuze uit:

0 = Geen toegang
1 = Toegang; noodzakelijk in verband met uitoefening van mijn functie, taken of verantwoordelijkheid.
2 = Toegang; geen verband met uitoefening van mijn functie.

School en Organisatie

Vink uw keuze aan, of vink '?' aan indien onbekend.

Financiële- en organisatiegegevens	?	0	1	2
Balans/winst- en verliesrekening				
Bank- en betaalgegevens				
Salarisadministratie				
Overeenkomsten				
Belastingdienst				
Subsidies				
Overheid				
Overige				

Personeelsgegevens	?	0	1	2
Personeelsadministratie				
Personeelsbeoordelingssysteem				
Sollicitantengegevens				
Ontslag- en uitkeringsgegevens				
Pensioen en vervroegde uittreding				

Bijzondere personeelsgegevens	?	0	1	2
Godsdienst of levensovertuiging				
Ras				
Nationaliteit				
Seksuele leven/voorkeur				
Politieke voorkeur				
Gezondheid/medische gegevens				
Vakbondslid				
Demografische klasse/indeling				

Overige personeelsgegevens	?	0	1	2
NAW gegevens				
Geboortedatum en -plaats				
Financiële gegevens				
Privé telefoon/e-mail				
Identiteitsgegevens (BSN, paspoort, rijbewijs, etc.)				
Overige				

Leveranciers

Vink uw keuze aan, of vink '?' aan indien onbekend.

Leveranciers	?	0	1	2
Bank- en betaalgegevens				
Inkoopgegevens				
Leveranciersbestanden (NAW)				

Inkoopinformatiesysteem (IIS)				
Inkoopplannen				
Inkoopvoorwaarden				
Overige				

ICT en beveiligingstoepassingen

Vink uw keuze aan, of vink '?' aan indien onbekend.

ICT en beveiligingstoepassingen	?	0	1	2
Inlogaccounts leerkrachten/collega's				
Toegangsaccounts ICT netwerk				
Toegangsaccounts inbraakbeveiliging				
(Software) licentieovereenkomsten				
Pasjessysteem/kaart-managementsysteem				
Toegangscontrole huisvesting				
Presentie/absentieregistratiesysteem				
Office 365 accounts				
Overige				

Dienstverlening en registratie

Vink uw keuze aan, of vink '?' aan indien onbekend.

Dienstverlening en registratie	?	0	1	2
Aansluitgegevens gas, water, elektra, telecommunicatie (ook mobiel en abonnement(en)				
Marktonderzoek, websitebezoek, websiteaankoop, cookies, etc.				

Leerling gegevens

Vink uw keuze aan, of vink '?' aan indien onbekend.

Algemeen	?	0	1	2
NAW gegevens				
Geboortedatum en -plaats				
Nationaliteit				
Financiële gegevens ouders/leerlingen				
Wettelijk vertegenwoordiger				
Aard en verloop studieresultaten				
Studieadvies				
Inlogaccounts				
Rapportage naar vervolgonderwijs				
Leerlingen volgsysteem (LVS)				
Elektronische Leeromgeving (ELO)				
Pasjessysteem/kaartmanagementsysteem				
Presentie/absentieregistratiesysteem				
Office 365 accounts				
Systemen educatieve uitgeverijen				

Bijzondere leerling gegevens	?	0	1	2
Godsdienst of levensovertuiging				
Ras				
Seksuele leven/voorkeur				
Gezondheid/medische gegevens				
Demografische klasse/indeling				

Schoolbegeleidingsdienst/schoolmaatschappelijk werk				
Acties rondom de leerling				
Specifiek schoolgegevens (bijvoorbeeld mentor en/of zorgcoördinator)				
Informatie inzake pesten				
Informatie inzake hulpverleningscontracten/overeenkomst				
Extern aangemelde informatie inzake begeleiding				

Hoe krijgt u toegang tot bovenstaande gegevens?

Vink JA of NEE aan.

Toegangsmogelijkheden	JA	NEE
Vrije toegang zonder enige beperking		
Via inlogaccount met wachtwoord		
Token/MFA (multi factor authentication)		
Versleuteld bijvoorbeeld met behulp van SSL (HTTPS verbinding)		

Waar staan of worden de bovenstaande gegevens opgeslagen?

Vink JA of NEE aan.

Werk	JA	NEE
Server		
Cloud		
Werkstation		
Laptop		
Datadrager (USB/DVD/Harddisk, etc.)		

Privé	JA	NEE
Server		
Cloud		
Werkstation		
Laptop		
Datadrager (USB/DVD/Harddisk, etc.)		

Overige vragen

Vink JA of NEE aan, of vink '?' aan indien onbekend.

Overige vragen	?	JA	NEE
Is de privacygevoelige informatie voorzien van een wachtwoord en encryptie (dataversleuteling)?			
Is bij uw leidinggevende bekend tot welke gegevens u toegang krijgt of heeft?			
Heeft u instructies gekregen inzake het privacy- en ICT gebruiksbeleid dat binnen uw organisatie van toepassing is?			
Bent u in kennis gesteld omtrent de inhoud van de 'Medewerkersovereenkomst intern privacy- en ICT beheer'.			