Handboek Privacy

Stichting Islamitisch Onderwijs Noord-Holland

April 2023

Versie: 1.0

Besproken en vastgesteld in MR op	
Voorzitter MR:	Handtekening:

Inhoudsopgave

Inleiding **3**

Deel A **5**

Privacyreglement 8
Gedragscode veilig gebruik ICT-middelen en persoonsgegevens 8
A1: Waar en hoe bewaar ik persoonsgegevens? 9
A2: Hoe en wat communiceer ik online via e-mail en sociale media? 11
A3: Hoe houd ik 'indringers' op afstand? 13
A4: Wanneer moet ik iets met toestemming regelen? 15
A5: Waar moet ik op letten bij het uitwisselen van persoonsgegevens? 17
A6: Wat moet ik regelen als ik werk op mijn eigen device (pc, laptop, tablet, smartphone)? 20
A7: Hoe ga ik om met vragen en klachten over privacy? 21
A8: Wat moet ik weten over datalekken? 22

Deel B **23**

B1: Welke rollen en verantwoordelijkheden t.a.v. IBP zijn er binnen SIO Noord-Holland belegd? 24
B2: Wat moet ik met ouders/verzorgers en medewerkers regelen rondom privacy? 25
B3: Wat moet ik weten als het gaat om het verlenen van toegang tot persoonsgegevens? 26
B4: Welke afspraken moet ik maken met mijn medewerkers in het kader van privacy? 27
B5: Wat moet ik afspreken met medewerkers in het kader van geheimhouding? 28
B6: Welke afspraken maak ik over devices die in bruikleen worden gegeven? 29
B7: Wat moet ik weten over datalekken? 30
B8: Hoe lang moet ik persoonsgegevens bewaren? 31
B9: Wat moet ik weten over externe partijen die namens de school persoonsgegevens verwerken? 32
B10: Welke technische maatregelen moet ik geregeld hebben binnen de school? 33
B11: Hoe kan ik aantonen dat ik IBP op orde heb? 34

Bijlagen **35**

1. Toegangsbeleid ParnasSys 36
2. Toelichting voor toestemming gebruik beeldmateriaal 39
3. Geheimhoudingsverklaring 42
4. Aanvraagformulier digitaal lesmateriaal 43
5. Model Gebruikersovereenkomst voor device in bruikleen bij medewerkers 44
6. Model Gebruikersovereenkomst voor device in bruikleen bij leerlingen 46
7. Voorbeeldprotocol ICT en Sociale media voor leerlingen 48
8. Tekst voor op de website en/of in de schoolgids 49
9. Informatiebeveiliging en Privacybescherming (IBP) 50
9. Privacyreglement SIO Noord-Holland 62
10. Procedure melden beveiligingsincidenten en datalekken SIO Noord-Holland 76

Inleiding

Informatie en ICT zijn noodzakelijk in de ondersteuning van het onderwijs. Omdat we binnen SIO Noord-Holland met persoonsgegevens (van medewerkers, leerlingen en anderen) werken, is privacywetgeving daarop van toepassing. Deze wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen op het gebied van informatiebeveiliging en privacy (afgekort: IBP) genomen moeten worden om de persoonsgegevens te beschermen. Hiervoor is binnen SIO Noord-Holland een IBP-beleid opgesteld.

Dit handboek is bedoeld om op schoolniveau uitvoering te geven aan het IBP-beleid. Het is bedoeld als informatiebron voor alle medewerkers van SIO Noord-Holland. In dit handboek staan de afspraken die we met elkaar hebben gemaakt over informatiebeveiliging en privacy.

Het handboek omvat met name de organisatorische maatregelen. Deze maatregelen nemen we niet alleen omdat de wet dat voorschrijft, maar ook op basis van de normen en waarden die wij vanuit onze visie op onderwijs met elkaar delen en uitdragen.

In het handboek wordt het IBP-beleid concreet gemaakt en uitgewerkt in aanvullende documenten. Een aantal van deze documenten zijn vanuit de Algemene Verordening Gegevensbescherming verplicht. Het IBP-beleid en de aanvullende documenten zijn voor iedereen van toepassing. Enkele documenten zijn echter voor schoolleiders van groter belang. Daarom is het handboek opgedeeld in twee delen:

Deel A - Medewerkers

Dit deel bevat de algemene informatie die voor alle medewerkers van SIO Noord-Holland van belang is. Van alle medewerkers wordt verwacht dat zij op de hoogte zijn van de afspraken die hierin vermeld staan en hier ook naar handelen (uiteraard voor zover deze in hun functie van toepassing zijn).

Deel B – Schoolleiding

In dit deel is informatie terug te vinden die vooral van belang is voor de schoolleiding. Het geeft antwoord op de vraag: hoe zorg ik ervoor dat informatiebeveiliging en privacy op mijn school goed geregeld is?

Deel A en B beginnen met een opsomming van de onderdelen of vragen, waarop doorgeklikt kan worden om snel de antwoorden te kunnen vinden.

Bijlagen

Hierin zijn richtlijnen, relevante informatie en formulieren terug te vinden die binnen SIO Noord-Holland gebruikt worden

Vastgestelde procedures en beleidsdocumenten

De vastgestelde procedures en beleidsdocumenten rondom de AVG zijn ook opgenomen achter in het handboek, waaronder het IBP-beleid, het privacyreglement en de procedure voor het melden van beveiligingsincidenten en datalekken.

Deel A

Informatie voor alle medewerkers

Aan de hand van onderstaande onderdelen worden in dit deel van het handboek de belangrijkste punten uitgewerkt en toegelicht.

- De Vijf vuistregels
- Privacyreglement
- Gedragscode veilig gebruik ICT-middelen en persoonsgegevens

Vijf vuistregels

Privacy is voor jou misschien een wat lastig en vaag begrip. Wat houdt dit precies in? Privacy gaat voor scholen over de bescherming van gegevens over leerlingen, hun ouders/verzorgers en medewerkers. Privacybescherming wordt geregeld in de Algemene Verordening Gegevensbescherming (AVG).

Wat zijn persoonsgegevens?

Gegevens die direct over iemand gaan, ofwel naar deze persoon te herleiden zijn. Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Bepaalde gevoelige gegevens zoals iemands ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd. Binnen SIO Noord-Holland worden gegevens van zowel leerlingen, ouders als medewerkers verwerkt. Welke gegevens dit zijn en voor welke doeleinden deze worden verwerkt staat omschreven in het privacyreglement.

In onderstaande vuistregels van Kennisnet worden de belangrijkste uitgangspunten voor het verantwoord omgaan met persoonsgegevens samengevat. Binnen SIO Noord-Holland spreken we met elkaar af dat we altijd nagaan of we aan al deze vuistregels voldoen bij het verzamelen en verstrekken van persoonsgegevens aan de hand van de volgende vragen.

1. Doel en doelbinding
Heb ik vooraf een doel voor de verwerking van persoonsgegevens vastgesteld? Worden de persoonsgegevens alleen gebruikt voor dat doel dat ik vooraf heb vastgelegd?

2. Grondslag
Is er minimaal een wettelijke grondslag voor de verwerking? Er is een wettelijke grondslag als…

- er een wettelijke plicht bestaat om deze gegevens te verstrekken. Bijv. voor bekostiging, inspectie, overdrachtsdossier, etc.;
- er toestemming is verkregen van de ouders/verzorgers. Bijv. voor de begeleiding van een leerling door externe onderwijsspecialisten, foto's op website, etc.;
- de partij een publiekrechtelijke taak heeft. Bijv. de uitwisseling van informatie met samenwerkingsverbanden;
- dit nodig is voor het uitvoeren van een overeenkomst met de ouders/verzorgers. Bijv. het verzorgen van onderwijs aan kinderen in het kader van de inschrijving (= overeenkomst);
- er sprake is van een gerechtvaardigd belang, zoals het goed laten werken van digitale leermiddelen. Bijv. voor Basispoort en educatieve uitgeverijen.

Zie onderdeel A5 voor de grondslagen voor de meest voorkomende uitwisselingen/verwerkingen.

3. Dataminimalisatie
Gebruik ik alleen die gegevens die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? Kan ik met minder of bijvoorbeeld anonieme gegevens werken? Bewaar ik de gegevens niet langer dan nodig?

4. Transparantie
Heb ik de leerling of zijn ouders vooraf helder geïnformeerd over het doel van de gegevensverwerking? Heb ik uitgelegd welke gegevens worden gebruikt en met wie deze worden gedeeld?

5. Data-integriteit
Kloppen de persoonsgegevens die ik gebruik nog steeds? Zijn de gegevens op het juiste moment, op de juiste plaats en voor de juiste mensen beschikbaar? Heb ik onjuiste gegevens gecorrigeerd of verwijderd?

Privacyreglement

Het privacyreglement maakt duidelijk aan de personen van wie gegevens worden verzameld (ook wel betrokkenen genoemd) waarvoor de verzamelde gegevens nodig zijn en welke gegevens dit zijn (doel en doelbinding uit de vuistregels). Hiermee voldoet SIO Noord-Holland aan haar informatieplicht. Het privacyreglement is door ouders en medewerkers in te zien via de website www.sionoord-holland.nl/privacy.

Het privacyreglement is ook opgenomen in de bijlage van het handboek. Ouders worden via het inschrijfformulier en via de website van de scholen gewezen op het privacyreglement

Gedragscode veilig gebruik ICT-middelen en persoonsgegevens

Voor een veilig schoolklimaat en het voorkomen van boetes in het kader van privacywetgeving, is het belangrijk dat alle medewerkers zorgvuldig omgaan met persoonsgegevens. Daarom is er een gedragscode opgesteld waaraan alle medewerkers van SIO Noord-Holland zich dienen te houden.

In deze gedragscode staan afspraken over de volgende onderdelen:

A1: Waar en hoe bewaar ik persoonsgegevens?

A2: Hoe en wat communiceer ik online via e-mail en sociale media?

A3: Hoe houd ik indringers op afstand?

A4: Wanneer moet ik iets met toestemming regelen?

A5: Waar moet ik op letten bij het uitwisselen van persoonsgegevens?

A6: Wat moet ik regelen als ik werk op mijn eigen device (pc, laptop, tablet, smartphone)?

A7: Hoe ga ik om met vragen en klachten over privacy?

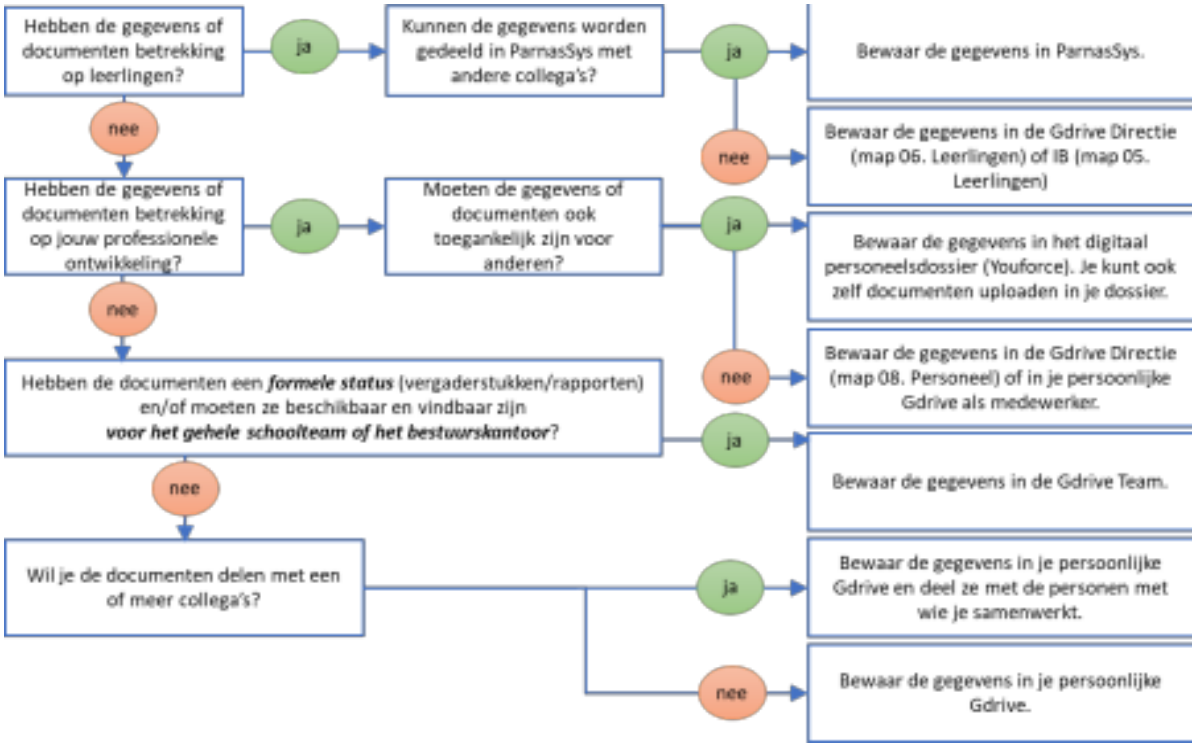
A8: Wat moet ik weten over datalekken?

A1: Waar en hoe bewaar ik persoonsgegevens?

Binnen SIO Noord-Holland worden vertrouwelijke gegevens van zowel leerlingen als personeel verwerkt. Bij leerlingen dient hierbij gedacht te worden aan adres- en contactgegevens, toetsgegevens, absentie, notities, maar ook medische en andere 'gevoelige' informatie indien dit relevant is voor de onderwijsbegeleiding. Van het personeel worden adres- en contactgegevens bijgehouden, alsmede salarisgegevens en ziekteverzuim. Daarnaast wordt in de administratie en communicatie van de scholen foto- en videomateriaal gebruikt van zowel personeel als leerlingen.

Om ervoor te zorgen dat we binnen de school onze documenten en gegevens (data) overzichtelijk en veilig opgeslagen hebben, zijn er afspraken over wat we waar bewaren. Op deze manier zijn documenten niet alleen eenvoudiger terug te vinden, maar kunnen ze ook beter afgeschermd en geback-upt worden.

In het schema hieronder kun je nagaan op welke plek je gegevens en documenten moet bewaren.



De mappen in de Gdrive zijn toegankelijk voor specifieke functies. Zolang medewerkers bepaalde informatie of gegevens nodig hebben voor het uitvoeren van hun functie, mogen zij toegang hebben tot deze gegevens, mits zij in dienst zijn. Op documentniveau kunnen eventueel (tijdelijke) leesrechten gegeven worden aan specifieke medewerkers indien zij hiertoe toegang nodig hebben.

- Sla persoonsgegevens alleen op daarvoor afgesproken plaatsen op. Opslaan van persoonsgegevens in een public Cloud omgeving, zoals een persoonlijke Dropbox, is niet toegestaan. Ook het opslaan op een USB-stick is niet toegestaan. Zie A1 voor de afgesproken bewaarplaatsen binnen SIO Noord-Holland.
- Verwerk persoonsgegevens zoveel mogelijk in de daarvoor afgesproken systemen. Leerlinggegevens worden zo veel mogelijk ingescand en in ieder geval digitaal opgeslagen in ParnasSys, zodat ze daar geraadpleegd kunnen worden. Dit geldt ook voor gegevens die via ouders/verzorgers en/of externen worden ontvangen. Gegevens over medewerkers worden bewaard in Youforce, tenzij dit op papier bewaard moet blijven vanwege wettelijke verplichtingen.
- Gebruik voor het verwerken van persoonsgegevens een computer die voldoet aan de beveiligingseisen van SIO Noord-Holland. Moet je (documenten met) persoonsgegevens downloaden en bewerken op je 'eigen' computer? Doe dit dan alleen op een computer (laptop, smartphone) die voldoet aan de beveiligingseisen van SIO Noord-Holland. Lees hiervoor de afspraken in onderdeel A6. Verwijder de persoonsgegevens na gebruik van je computer. Zorg ervoor dat anderen (bijv. familieleden) niet bij jouw werkbestanden kunnen komen.
- Formuleer gegevens die je vastlegt over een persoon zorgvuldig en professioneel. Ouders hebben het recht om het dossier van hun kind(eren) in te zien. Zorg ervoor dat de gegevens zodanig zijn geformuleerd dat dit ingezien kan worden en aansluit bij je houding als onderwijsprofessional.
- Ga na welke afspraken er binnen SIO Noord-Holland zijn gemaakt, voordat je gegevens uitwisselt met derden. Wanneer je gegevens uitwisselt met collega's of andere organisaties, zoals bijvoorbeeld de logopedist, een arts, de jeugdzorg, een schoolbegeleidingsdienst of een andere school, kijk dan goed welke afspraken hierover zijn gemaakt binnen de school. In de meeste gevallen is toestemming nodig van de ouders. Lees in onderdeel A5 wanneer dit het geval is. Zorg dat je de toestemming ook schriftelijk vastlegt, dit kan ook per mail.

A2: Hoe en wat communiceer ik online via e-mail en sociale media?

Binnen SIO Noord-Holland wordt er, naast de fysieke contactmomenten, met ouders en andere betrokkenen buiten de school gecommuniceerd via e-mail, ParnasSys, Parro, de website, het ouderportaal, de nieuwsbrief en/of via sociale media. SIO Noord-Holland wil dat kinderen zich veilig voelen op school. Daarnaast heeft SIO Noord-Holland de wettelijke verplichting om zorgvuldig om te gaan met de verwerking van persoonsgegevens. Het gebruik van digitale communicatiemiddelen sluit aan bij de eigentijdse manier waarop SIO Noord-Holland betrokkenen wil informeren en toegankelijk wil zijn. De scholen binnen SIO Noord-Holland zorgen ook digitaal voor een veilig klimaat en communiceren met personeelsleden, leerlingen en ouders/verzorgers hoe zij dit doen. SIO Noord-Holland stelt aan alle medewerkers een mailaccount ter beschikking en een bijbehorende mailbox voor het uitoefenen van de werkzaamheden. Voor het communiceren via e-mail, sociale media en andere kanalen, gelden de volgende regels:

- Van de medewerkers binnen SIO Noord-Holland wordt verwacht dat zij op een professionele manier communiceren en handelen, dat wil zeggen:
  - Geen eigen online communicatiemiddelen (privé e-mail, sociale media) gebruiken voor het contact met ouders/verzorgers of leerlingen vanuit hun rol als professional;
  - Dat de inhoud van e-mails functioneel en professioneel moet zijn;
  - Niet op persoonlijke titel communiceren vanuit hun rol als professional;
  - Geen privéberichten versturen via een account van SIO Noord-Holland;
  - Geen online discussie voeren met ouders/verzorgers of leerlingen;
  - Zich niet negatief uitlaten over de school, ouders/verzorgers of leerlingen.

- Deel nooit informatie via sociale media over (individuele) leerlingen. Doe dit vooral in persoon of desnoods via de telefoon. Wat je communiceert via sociale media kan makkelijk anders worden geïnterpreteerd door de lezer als je hier niet alert op bent.

- Ga voordat je foto's of video's publiceert waar leerlingen herkenbaar op te zien zijn, na of ouders hiervoor toestemming hebben gegeven. Ouders moeten toestemming geven voor het publiceren van foto's en video's waarop leerlingen herkenbaar in beeld zijn gebracht. De toestemming moet schriftelijk vastgelegd zijn. Zie ook onderdeel A4.

- Zet e-mailadressen altijd in de BCC-regel als je naar (grote) groepen en/of mensen buiten SIO Noord-Holland een bericht verstuurt. Zo blijven de e-mailadressen van de groepsleden en externen afgeschermd en kunnen ze niet onbedoeld voor andere doeleinden (door anderen) gebruikt worden.

- *Stuur nooit zomaar een e-mailbericht door naar derden. Overleg indien nodig met de degene van wie je het bericht ontvangen hebt.* De afzender heeft de mail voor een ander persoon en met wellicht een ander doel geschreven. Door het door te sturen, kunnen anderen het bericht verkeerd interpreteren.

- Wanneer je een bericht stuurt met belangrijke en/of gevoelige informatie naar (een groep) ouders/verzorgers laat dit dan nalezen door een collega. Een foutje is snel gemaakt en bovendien kan een ander je boodschap anders interpreteren dan jij het bedoeld hebt.

- Maak gebruik van een link naar een document om persoonsgegevens uit te wisselen met collega's of verwijs naar de

vindplaats (in ParnasSys). Verstuur nooit persoonsgegevens per mail, maar verstuur een link met de vindplaats van de benodigde gegevens in ParnasSys. Wissel persoonsgegevens nooit uit via een USB-stick.

A3: Hoe houd ik 'indringers' op afstand?

Niet alle informatie is bestemd voor iedereen. Wees je hiervan bewust, zowel in de klas als daarbuiten. Weet hoe je de gevaren van internet kunt herkennen en hoe je daarmee omgaat. Om indringers op afstand te houden heeft SIO Noord-Holland de volgende afspraken vastgelegd:

Wachtwoorden

- Laat je wachtwoorden in ParnasSys of andere systemen met persoonsgegevens niet onthouden door je internetbrowser. En schrijf je logingegevens nooit op. Zonder dat je er erg in hebt, klik je de optie 'wachtwoord onthouden' in je browser aan. Heel makkelijk als je vaak moet inloggen, maar iemand anders die jouw device gebruikt kan dan dus ook heel makkelijk inloggen. Kijk hier voor een tip om een sterk wachtwoord te kiezen dat goed te onthouden is of gebruik een wachtwoordkluis (bijv. Lastpass.com).
- Houd je logingegevens altijd voor jezelf, ook al vragen anderen je om ze te delen. Je login is in feite een sleutel om toegang te krijgen tot de informatie die alleen voor jou toegankelijk moet zijn. Daarnaast herkent het systeem jou door je login, zodat het kan bijhouden wie welke gegevens heeft toegevoegd of gewijzigd. Deel je logingegevens dus nooit met anderen.
- Zet je digibord op freeze als je wachtwoorden intoetst of persoonsgegevens in je scherm ziet staan. En zorg dat niemand meekijkt als jij je wachtwoord intoetst. Voordat je het weet zien leerlingen gevoelige gegevens of kunnen ze aan de hand van je afgekeken gebruikersnaam en wachtwoord proberen in te loggen. Zet ook de notificatie-functie van je e-mail uit, zodat er tijdens je les geen meldingen op het bord binnen komen die leerlingen kunnen zien, maar niet voor hun ogen bestemd zijn.

Clean desk, clean screen

Meld je altijd af als je de computer onbeheerd achterlaat. En zorg ervoor dat er op je werkplek geen gevoelige informatie zichtbaar of voor het grijpen ligt, ook niet bij de printer.

Met de combinatie van de **Windows- en L-toets of CTRL+ALT+DEL** kun je makkelijk je pc of laptop vergrendelen. Maak er een gewoonte van om papieren op je bureau om te draaien. Zo voorkom je dat anderen informatie zien die niet voor hen is bedoeld. (Clean desk, clean screen). Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan. Haal overbodig geworden papieren documenten met persoonsgegevens erop, altijd door de papierversnipperaar.

Overige

- Bewaar onbeheerde laptops of tablets altijd op een veilige (afgesloten) plek, zeker tijdens vakantieperiodes. Het is een open deur, maar toch gebeurt het heel erg makkelijk. Maak elkaar er dus op attent als je een laptop of tablet onbeheerd ziet liggen. Als je computer gestolen wordt, heeft dat niet alleen gevolgen voor jou als werknemer, maar ook voor de school en de leerlingen. Meld dit dus altijd direct bij je leidinggevende.
- Klik alleen op linkjes en open alleen bijlagen in e-mails van betrouwbare afzenders en pas op met het downloaden van bestanden. Virussen kunnen makkelijk worden binnengehaald via (phishing)mails. In het criminele circuit is dit een veelgebruikte methode om aan jouw gegevens of die van anderen te komen. Ook kunnen de gegevens op je computer op deze manier versleuteld worden (ransomware).

- Zorg er bij vertrouwelijke (telefonische) gesprekken voor dat er niet kan worden meegeluisterd. Trek je even terug als een gesprek een vertrouwelijk karakter heeft of krijgt.
- Meld het direct als:
  - Je laptop, tablet of telefoon met persoonsgegevens is gestolen.
  - Je USB-stick met persoonsgegevens is kwijtgeraakt.
  - Je niet meer bij je bestanden kunt, omdat je een virus hebt.
  - Je logingegevens van bijvoorbeeld ParnasSys of persoonsgegevens in handen van anderen zijn gekomen (of als je dit niet kunt uitsluiten).

Meld dergelijke voorvallen direct via privacy@sionoord-holland.nl in verband met de meldplicht datalekken. Zie onderdeel A8 voor meer informatie over datalekken.

A4: Wanneer moet ik iets met toestemming regelen?

Je mag persoonsgegevens verwerken als je daar een wettelijke grondslag voor hebt. De grondslag toestemming is in een aantal gevallen van toepassing. Vraag je om toestemming voor het verwerken van persoonsgegevens? Dan moet de manier waarop ouders of leerlingen toestemming geven aan drie voorwaarden voldoen:

- Je moet expliciet vragen om toestemming. De vraag mag niet verborgen zijn in schoolregels, maar wordt geregeld in een apart toestemmingsformulier of via een app. Het credo: wie zwijgt stemt toe, gaat niet op; de betrokkene moet actief toestemming verlenen (geen reactie = geen toestemming)
- Het moet duidelijk zijn waarvoor toestemming gegeven wordt, met wie gegevens gedeeld worden en voor welk doel.
- Betrokkenen moeten er bij het vragen van toestemming op gewezen worden dat zij hun toestemming te allen tijde kunnen intrekken.

De meest voorkomende toestemmingen worden via de app Parro geregeld. Dit kan via ParnasSys ingesteld worden. In onderdeel B2 (voor de schoolleiding) vind je hierover meer informatie.

Beeldmateriaal

In de nieuwe privacywetgeving zijn de regels rondom het publiceren van beeldmateriaal aangescherpt. Ouders moeten altijd toestemming geven voor het gebruik van beeldmateriaal. Het moet voor ouders/verzorgers duidelijk zijn voor welk gebruik van het beeldmateriaal ze toestemming geven, bijvoorbeeld voor het gebruik in de website, een nieuwsbrief of de schoolgids.

Ouders hebben altijd de mogelijkheid deze toestemming weer in te trekken of op een later moment alsnog toestemming te geven. De pasfoto in het leerlingdossier is een uitzondering, hiervoor is geen toestemming nodig.

Uiteraard zijn er in de school ook ouders die foto's of video's maken bijvoorbeeld bij feestelijke gelegenheden. De school moet een veilige omgeving zijn voor alle kinderen (en hun ouders/verzorgers) en zij moeten niet het risico lopen ongewenst gefotografeerd te worden. Het is echter lastig om het maken van beeldopnamen door ouders/verzorgers te verbieden. SIO Noord-Holland wijst ouders in onder andere de schoolgids erop verantwoord om te gaan met zelfgemaakt beeldmateriaal waarop ook andere kinderen staan dan de eigen kinderen. Lees in de bijlage meer over toestemming bij het gebruik van beeldmateriaal.

Uitwisseling persoonsgegevens

Wanneer je gegevens van leerlingen uit wil wisselen met externen, zoals bijvoorbeeld een arbo- of schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Geef de gegevens daarom – waar mogelijk – mee met de ouders, zodat zij zelf de gegevens kunnen uitwisselen met externe hulpverleners. Lees in onderdeel A5 meer over de uitwisseling van persoonsgegevens.

Online diensten

Voor het gebruik van bepaalde online diensten door leerlingen binnen of buiten de school moeten ouders ook toestemming verlenen. Dit betreft alleen online diensten die ook buiten de school om in het maatschappelijk verkeer gebruikt kunnen worden. Voor e-mail, digitale leeromgevingen of leermiddelen waarvoor door de school zelf een account wordt verstrekt is dus geen toestemming nodig. Dit betekent dat wanneer leerlingen in opdracht van de school gebruik moeten maken van een (privé)account voor bijvoorbeeld Pinterest of Instagram of Facebook, ouders hier vooraf toestemming voor moeten geven. Deze online diensten kunnen immers ook los van de school worden gebruikt.

A5: Waar moet ik op letten bij het uitwisselen van persoonsgegevens?

Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een Arbo- of schoolarts, jeugdzorg of een schoolbegeleidingsdienst, dan is het vaak nodig om toestemming te vragen van ouders of medewerkers. Zorg dat je de toestemming registreert en houd daarbij ook rekening met de verdeling van het ouderlijk gezag. Kijk hieronder in de tabel met welke partijen je gegevens mag uitwisselen en op welke manier.

Verstrekking aan	Doel	Uitwisseling toegestaan	Grondslag (zie vuistregels)	Wijze waarop
Dienst Uitvoering Onderwijs	Bekostiging*	Ja	Wettelijke plicht *(art. 69 e.v. Wet PO)*	Koppeling ParnasSys
Educatieve uitgeverijen en Basispoort	Gebruik digitale leermiddelen	Ja	Gerechtvaardigd belang	Koppeling ParnasSys
Apps en sociale media	Onderwijs	Ja	Toestemming	Handmatige invoer
Basisscholen of scholen voor voortgezet onderwijs	Overdracht leerlingdossier (na aanmelding) *	Ja	Wettelijke plicht *(art. 42 Wet PO)*	Koppeling OSO
Externe Onderwijsspecialisten	Zorgbegeleiding van een leerling	Ja	Toestemming	Verstrekken account
Stagiaires	Opleiden	Ja	Uitvoeren overeenkomst	Verstrekken account
Samenwerkingsverband	Toelaatbaarheidsverklaring afgeven*	Ja, zie ook: https://passendonderwijsenprivacy.nl	Wettelijke plicht of toestemming *(art. 18a e.v. Wet PO)*	n.t.b.
Activiteiten - commissie	Innen ouderbijdrage	Ja	Gerechtvaardigd belang	n.t.b.
GGD/JGZ	Bezoek schoolarts	Nee, tenzij dit niet uit BRON geleverd kan worden.	Algemeen belang	n.v.t.
Inspectie van het onderwijs	Toezicht*	Ja	Wettelijke plicht *(Wet PO en Wet op het onderwijstoezicht)*	Via Internet School Dossier (ISD)
Administratiekantoor	Salarisadministratie en HR-management	Ja	Gerechtvaardigd belang of uitvoeren	n.t.b.
Accountant	Controle	Ja	Wettelijke plicht	n.t.b.

Verstrekking aan	Doel	Uitwisseling toegestaan	Grondslag (zie vuistregels)	Wijze waarop
Dienst Uitvoering Onderwijs	Bekostiging*	Ja	Wettelijke plicht *(art. 69 e.v. Wet PO)*	Koppeling ParnasSys
Educatieve uitgeverijen en Basispoort	Gebruik digitale leermiddelen	Ja	Gerechtvaardigd belang	Koppeling ParnasSys
			(art. 171 e.v. Wet PO)	
Leerplicht Gemeente	Controle verzuim	Ja	Wettelijke plicht *(Leerplichtwet)*	Verzuimloket
Ouderraad	Ouderbetrokkenheid	Ja	Gerechtvaardigd belang	n.t.b.
Arbodienst	Personeelszorg	Ja	Wettelijke plicht *(Arbeidsomstandig hedenwe t)*	n.t.b.
Bibliotheek	Onderwijs	Ja	Toestemming	n.t.b.
Nationale Nederlanden (WGA)	Verzekering	Ja	Toestemming	n.t.b.
Publiceren beeldmateriaal	PR en ouderbetrokkenheid	Ja	Toestemming	n.t.b.

* Wettelijk verplicht

Gemeente en leerplichtambtenaren

De gemeente vraagt soms om informatie van leerlingen voor gemeentebeleid. Ook belt de leerplichtambtenaar soms voor een specifiek geval. Hoewel dit officiële instanties zijn, hebben zij niet altijd recht op informatie. De informatie die de gemeente nodig heeft en waar zij recht op heeft, krijgt zij via DUO en hoeft de school dus niet aan te leveren. Dit geldt dus ook voor de GGD. Overleg met de directeur, voordat je gegevens uitwisselt met deze en andere organisaties.

Samenwerkingsverbanden

Voor de uitwisseling van leerlinggegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Hiervoor kun je terecht bij de zorgbegeleider. Kijk op http://steunpuntpassendonderwijs-vo.nl/ voor meer informatie over privacy en Samenwerkingsverbanden, ook voor basisscholen.

Inspectie van het onderwijs

De inspectie mag alleen persoonsgegevens verwerken als dat voor haar wettelijke taken noodzakelijk is. In de voorbereiding van een schoolbezoek of bij het uitvoeren van onze toezichttaken vraagt de inspectie om documenten aan te leveren. Deze gegevens dienen zo veel mogelijk geanonimiseerd aangeleverd te worden. In uitzonderlijke gevallen heeft de inspectie voor het uitvoeren van hun

toezicht- en handhavingstaken wel persoonsgegevens nodig. Documenten die persoonsgegevens bevatten, moeten aangeleverd worden via het ISD (Internet Schooldossier). Het ISD kent een goede beveiliging. In het ISD kan aangevinkt worden dat het om persoonsgegevens gaat, zodat de Inspectie het op een juiste manier kan verwerken.

Vragen om informatie via de telefoon

Geef nooit zomaar gegevens door via de telefoon, als iemand belt om navraag te doen over een leerling of medewerker. Ook dan is het weer belangrijk om te controleren of diegene wel die gegevens mag krijgen. Vraag altijd of de persoon het verzoek via de mail wil sturen. Dit geeft je de mogelijkheid om navraag te doen en uit te zoeken of de gegevens verstrekt mogen worden. Overleg bij twijfel met je leidinggevende.

A6: Wat moet ik regelen als ik werk op mijn eigen device (pc, laptop, tablet, smartphone)?

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor SIO Noord-Holland worden uitgevoerd. SIO Noord-Holland is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de ICT-middelen van de school. Voor eigen devices, ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen, zodat persoonsgegevens goed beschermd zijn:

- Gebruik geen USB-sticks voor de uitwisseling van persoonsgegevens of andere informatie van SIO Noord-Holland.
- Beveilig het eigen device met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode van minimaal 4 tekens.
- Scherm e-mail en andere apps of online toepassingen van SIO Noord-Holland op het eigen device af met een apart wachtwoord.
- Zorg dat e-mail en andere apps of online toepassingen niet toegankelijk zijn voor andere gebruikers.
- Sla geen bestanden die persoonsgegevens bevatten lokaal op het eigen device op (bijv. op de harde schijf), maar alleen op de daarvoor aangewezen bewaarplaatsen van SIO Noord-Holland.
- Zorg ervoor dat het eigen device is voorzien van antivirussoftware die up-to-date gehouden wordt.
- Houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks).
- Verwerk persoonsgegevens van SIO Noord-Holland niet via een openbaar Wifi-netwerk.
- Versleutel alle persoonsgegevens, met betrekking tot SIO Noord-Holland als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden.
- Scheid (versleutelde) persoonsgegevens met betrekking tot SIO Noord-Holland en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen device.
- Vergrendel het device bij het verlaten van de werkplek (Windowstoets+L).
- Sla wachtwoorden niet op in de browser.

SIO Noord-Holland mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van SIO Noord-Holland moet de medewerker aantonen dat de bovenstaande maatregelen worden toegepast.

A7: Hoe ga ik om met vragen en klachten over privacy?

Het is belangrijk om klachten of vragen over privacy serieus te nemen. Om deze goed te beantwoorden is het nodig om kennis en expertise te hebben op het gebied van privacy. Vandaar dat we binnen SIO Noord-Holland hier een centraal punt voor in hebben gericht, deze is te benaderen via: privacy@sionoord-holland.nl

Wettelijk gezien heeft iedereen, alle betrokkenen, van wie SIO Noord-Holland persoonsgegevens verwerkt, bepaalde rechten als het gaat om hun persoonsgegevens. Deze rechten zijn onder andere:

- Inzage en opvragen – een kopie van alle gegevens die over die persoon zijn verzameld binnen SIO Noord-Holland
- Rectificatie – als blijkt dat de gegevens die zijn verzameld onjuist of onvolledig zijn, dan heeft die persoon het recht om deze gegevens te laten aanvullen of corrigeren
- Wissen – SIO Noord-Holland kan verplicht zijn om gegevens onder bepaalde omstandigheden te wissen als de persoon die om inzage heeft gevraagd dit vraagt. Dit is niet altijd het geval, soms heeft SIO Noord-Holland bijvoorbeeld een wettelijke plicht om bepaalde informatie te verwerken en kan zij dit niet zomaar verwijderen. Dit zal per geval moeten worden bekeken.

Wil je inzage hebben in de gegevens die over jou zijn verzameld of je krijgt de vraag van een leerling of een ouder? Dan kan dat via de directeur van de school.

N.B. In het geval van klachten, bekijk dan ook de klachtenregeling van SIO Noord-Holland.

A8: Wat moet ik weten over datalekken?

Zijn er leerlinggegevens verloren gegaan? Is je laptop gestolen? Heb je last van een virus waardoor je niet meer bij je bestanden kunt? Of vertrouw je iets niet? Dan ben je verplicht dit zo snel mogelijk te melden bij je direct leidinggevende. Als er persoonsgegevens beschadigd of verloren zijn, of als de mogelijkheid bestaat dat iemand onbevoegd toegang heeft kunnen krijgen tot persoonsgegevens dan moet er mogelijk binnen 72 uur een melding gedaan worden bij de Autoriteit Persoonsgegevens in het kader van meldplicht datalekken.

We spreken van een datalek wanneer er persoonsgegevens (van leerlingen, hun ouders of medewerkers) in handen kunnen vallen van derden die geen toegang tot die gegevens zouden mogen hebben of wanneer er persoonsgegevens onbedoeld verloren zijn gegaan of onbedoeld zijn gewijzigd. Voorbeelden van datalekken zijn de volgende incidenten, waarbij persoonsgegevens betrokken zijn:

- Een e-mail die aan een verkeerd persoon geadresseerd is
- Een kwijtgeraakte USB-stick
- Inloggegevens die openbaar zijn geworden
- Een gestolen tablet
- Een gehackte computer
- Gestolen of zoekgeraakte documenten
- Onbedoeld gewijzigde gegevens

Het bevoegd gezag is eindverantwoordelijk voor de bescherming van persoonsgegevens van leerlingen en personeel en moet bepalen of er een melding gedaan moet worden bij de Autoriteit Persoonsgegevens. Wanneer er een datalek ten onrechte niet wordt gemeld, kan een hoge boete opgelegd worden.

Ben je dus (een device met) persoonsgegevens kwijtgeraakt of heb je onrechtmatigheden geconstateerd met betrekking tot de toegang tot persoonsgegevens? Meld dit dan direct via privacy@sionoord-holland.nl en/of bij je leidinggevende.

Bekijk hier de Procedure Melden Beveiligingsincidenten en Datalekken.

Deel B

Informatie voor de schoolleiding

Belangrijke vragen

Aan de hand van onderstaande vragen worden in dit deel van het handboek de belangrijkste punten uitgewerkt en toegelicht.

B1: Welke rollen en verantwoordelijkheden t.a.v. IBP zijn er binnen de schoolorganisatie belegd?

B2: Wat moet ik met ouders regelen rondom privacy?

B3: Wat moet ik weten als het gaat om het verlenen van toegang tot persoonsgegevens?

B4: Welke afspraken moet ik maken met mijn medewerkers in het kader van privacy?

B5: Wat moet ik afspreken met medewerkers in het kader van geheimhouding?

B6: Welke afspraken maak ik over devices die in bruikleen worden gegeven?

B7: Wat moet ik weten over datalekken?

B8: Hoe lang moet ik persoonsgegevens bewaren?

B9: Wat moet ik weten over externe partijen die namens de school persoonsgegevens verwerken?

B10: Welke technische maatregelen moet ik geregeld hebben binnen de school?

B11: Hoe kan ik aantonen dat ik IBP op orde heb?

B1: Welke rollen en verantwoordelijkheden t.a.v. IBP zijn er binnen SIO Noord-Holland belegd?

Bij het vaststellen en uitvoeren van het IBP-beleid zijn verschillende rollen en verantwoordelijkheden vastgesteld binnen SIO Noord-Holland. Het bestuur van SIO Noord-Holland hanteert hierbij het three lines of defence model om de governance te borgen.

De 1e lijn binnen dit model is cruciaal. Hierin is vastgelegd dat de locatie directeuren moeten toezien op het verantwoord omgaan met persoonsgegevens. Zij zien erop toe dat al hun teamleden handelen volgens het vastgestelde IBP-beleid en de daarbij behorende afspraken en procedures. De 2e lijn en 3e lijn worden ingevuld door respectievelijk de Privacy Officer en Functionaris Gegevensbescherming, in nauwe samenwerking met de beleidsgroep ICT.

In het IBP-beleid is dit verder schematisch vastgelegd. Zie het hoofdstuk Rollen verantwoordelijkheden in het IBP-beleid in de bijlage voor een omschrijving van de taken en verantwoordelijkheden.

B2: Wat moet ik met ouders/verzorgers en medewerkers regelen rondom privacy?

Privacyreglement

Ouders, leerlingen en medewerkers hebben het recht om te weten welke gegevens er van hen worden verzameld door de school en voor welke doeleinden. Met het privacyreglement voldoet SIO Noord-Holland aan zijn wettelijke informatieplicht, mits deze ook actief onder de aandacht van de ouders wordt gebracht. Daarom is het belangrijk dat alle scholen naar het privacyreglement verwijzen in hun schoolgids, inschrijfformulier en op hun website.

Toestemming ouders/verzorgers

Voor het gebruik van foto- en filmopnames van leerlingen is toestemming vereist. Hiervoor kan de app Parro gebruikt worden. In ParnasSys kan ingesteld worden waarvoor de ouders toestemming moeten geven via de app. Zie de afbeelding hieronder voor de toestemmingen die standaard uitgevraagd kunnen worden. Elke school maakt hierin een passende selectie en vult deze zonodig aan. Het is niet nodig om jaarlijks opnieuw toestemming te vragen. Het is daarentegen wel belangrijk om ouders jaarlijks (aan het begin van het nieuwe schooljaar) te herinneren aan de opgegeven voorkeuren in de app Parro.

Afbeelding: Toestemmingsvragen Parro

Toestemming medewerkers

Op school worden opnamen gemaakt tijdens verschillende gelegenheden. Ook medewerkers kunnen op deze foto's (en soms in video's) te zien zijn. Voor de publicatie hiervan wordt bij indiensttreding aan medewerkers om toestemming gevraagd. Deze toestemming geldt alleen voor foto's en video's die door of in opdracht van de school worden gemaakt. Het maken van foto's door ouders is binnen de school niet toegestaan. Het kan voorkomen dat andere ouders of leerlingen foto's maken tijdens schoolactiviteiten die buiten de school plaatsvinden. De school heeft daar geen invloed op. De school kan wel vragen aan ouders en leerlingen om terughoudend te zijn met het maken van foto's en video's en deze niet te delen via sociale media zonder toestemming.

Schoolfotograaf

Voor het maken van een klassenfoto heb je altijd toestemming nodig van de ouders van de leerlingen die erop komen. Vraag ouders dan ook tijdig toestemming voor het maken en delen van de klassenfoto via de app Parro. Heb je van een leerling geen toestemming voor de klassenfoto? Dan gaat hij of zij dus niet op de foto. In alle gevallen maakt de school afspraken met de schoolfotograaf over de aflevering. Er worden immers in opdracht van de school en onder schooltijd foto's gemaakt.

Kijk voor meer informatie over toestemming voor beeldmateriaal de toelichting in de bijlage.

B3: Wat moet ik weten als het gaat om het verlenen van toegang tot persoonsgegevens?

Niet alle medewerkers hebben toegang tot (alle) leerlinggegevens. Per rol is binnen SIO Noord-Holland vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat die rol nodig heeft om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien of wijzigen.

Directeuren zijn verantwoordelijk (per 1-10-2020) voor het instellen van de juiste rol en bevoegdheden (in Parnassys) voor elke medewerker.

B4: Welke afspraken moet ik maken met mijn medewerkers in het kader van privacy?

Voor alle medewerkers bij SIO Noord-Holland geldt dat zij handelen conform de afspraken zoals opgenomen in deel A van het handboek. Deel A van dit handboek is de praktische uitwerking van het IBP-beleid.

Regelmatig moet bewustwording rondom privacy op de agenda van de scholen staan. Bij nieuwe medewerkers vraagt dat nog eens extra aandacht. Elke medewerker moet immers op de hoogte zijn van het bestaan en de inhoud van dit handboek. Het moet voor hen duidelijk zijn dat ze met vragen terecht kunnen bij de directeur.

B5: Wat moet ik afspreken met medewerkers in het kader van geheimhouding?

SIO Noord-Holland neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Iedereen die werkzaamheden verricht in opdracht van SIO Noord-Holland en daarbij toegang krijgt tot persoonsgegevens (welke in beginsel altijd vertrouwelijk zijn) is verplicht tot geheimhouding daarvan. Voor vaste medewerkers en tijdelijke medewerkers is dit geregeld in de arbeidsovereenkomst.

In de bijlage is een geheimhoudingsverklaring opgenomen die is bedoeld voor “externen”. Deze geheimhoudingsverklaring is van toepassing op personen die (deels) binnen de school werkzaam zijn en toegang hebben tot persoonsgegevens, maar geen arbeidsovereenkomst met de school hebben. Je kunt dan denken aan stagiaires, vrijwilligers (ouders), ZZP’ers, ingehuurde specialisten, leveranciers enz.

Alleen als zij persoonsgegevens verwerken of vertrouwelijke informatie verwerken van leerlingen, medewerkers of de school moet er met hen een geheimhoudingsverklaring ondertekend worden.

B6: Welke afspraken maak ik over devices die in bruikleen worden gegeven?

De school leent afhankelijk van de functie of aard van de werkzaamheden mobiele devices uit aan (een deel van) haar medewerkers en leerlingen. Dit kan gaan om een smartphone, tablet, Chromebook of een andere laptop. De devices zijn voorzien van beveiliging, zodat gegevens goed beschermd zijn. De devices zijn - indien nodig - naast antivirus o.a. voorzien van back-upfunctie, encryptie en worden na inname weer opgeschoond.

Aanvullend hierop legt SIO Noord-Holland nog een aantal afspraken schriftelijk vast over het gebruik van het device wanneer deze in bruikleen wordt gegeven aan een medewerker. Deze afspraken zijn vastgelegd in de gebruikersovereenkomst voor **medewerkers** en **leerlingen** zoals weergegeven in de bijlage.

B7: Wat moet ik weten over datalekken?

De verwerkingsverantwoordelijke conformeert zich aan de meldplicht datalekken zoals deze in het IBP beleid zijn beschreven.

Er is een interne procedure aanwezig voor het afhandelen van beveiligingsincidenten en datalekken. Zie bijlage Procedure melden beveiligingsincidenten en datalekken SIO Noord-Holland.

B8: Hoe lang moet ik persoonsgegevens bewaren?

SIO Noord-Holland hanteert de wettelijke bewaartermijnen voor persoonsgegevens zoals hieronder aangegeven. Wanneer de bewaartermijn verstreken is, moeten de betreffende gegevens vernietigd worden.

De schooldirecteuren zijn verantwoordelijk om jaarlijks onderstaande persoonsgegevens op te schonen. Geadviseerd wordt om dit in de laatste weken te doen voor de zomervakantie. Het gaat hierbij om zowel de digitale als papieren dossiers van leerlingen en medewerkers. Voor de dossiers van medewerkers die bovenschools worden verwerkt, ligt de verantwoordelijkheid voor opschonen bij de personeelsfunctionaris. Het is van belang dat vertrouwelijke gegevens onleesbaar worden vernietigd, d.m.v. een versnipperaar of ingehuurde vernietigingsdiensten.

Het opschonen van de persoonsgegevens, zoals hieronder vermeld, geldt vanaf 1 oktober 2020.

Gegevens	Wettelijke bewaartermijn	Toegepaste bewaartermijn
Gegevens over verzuim en afwezigheid	Maximaal 5 jaar nadat een leerling is uitgeschreven	5 jaar nadat een leerling is uitgeschreven
Gegevens in- en uitschrijving (noodzakelijk voor berekening van bekostiging)	Maximaal 5 jaar nadat een leerling is uitgeschreven	5 jaar nadat een leerling is uitgeschreven
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school krijgt	7 jaar na afloop van het schooljaar waarop de bekostiging betrekking heeft	7 jaar na afloop van het schooljaar waarop de bekostiging betrekking heeft
Gegevens in het leerling dossier in ParnasSys	Voorlopig 5 jaar nadat een leerling is uitgeschreven tot hierover een definitieve uitspraak is.	5 jaar (nadat een leerling is uitgeschreven, voorlopig, tot hierover een definitieve uitspraak is)
Gegevens met betrekking tot bezwaar-, klachten- of gerechtelijke procedure.	Maximaal 5 jaar nadat leerling is uitgeschreven	5 jaar nadat leerling is uitgeschreven
Gegevens in personeelsdossier met betrekking tot fiscale bewaarplicht	Maximaal 7 jaar na uitdiensttreding	7 jaar na uitdiensttreding
Overige gegevens in het personeelsdossier	Maximaal 2 jaar na uitdiensttreding	2 jaar na uitdiensttreding
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk door personeel en leerlingen	Maximaal 6 maanden	6 maanden
Sollicitatiebrief, formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	Maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant, maximaal 2 jaar na uitdiensttreding voor benoemde collega.	4 weken zonder toestemming 1 jaar met toestemming 2 jaar na uitdiensttreding voor benoemde collega

B9: Wat moet ik weten over externe partijen die namens de school persoonsgegevens verwerken?

In de privacywetgeving is bepaald dat het schoolbestuur als Verwerkingsverantwoordelijke afspraken moet maken met alle leveranciers die in opdracht van de school persoonsgegevens verwerken in zogenaamde verwerkersovereenkomsten. Het gaat hierbij bijvoorbeeld om uitgevers van digitaal lesmateriaal, leveranciers van toetsen, onderwijsadviesdiensten, etc. Wanneer een school een contract afsluit met een nieuwe leverancier die persoonsgegevens verwerkt in opdracht van de school, zal er ook een verwerkersovereenkomst afgesloten moeten worden. Wanneer het een contract met meerdere scholen betreft, dan wordt dit bovenschools geregeld.

Voor het afsluiten van verwerkersovereenkomsten wordt gebruik gemaakt van de meest actuele model verwerkersovereenkomst, die te vinden is via: www.privacyconvenant.nl

Om een goed beeld te krijgen van het digitaal lesmateriaal maakt SIO Noord-Holland gebruik van een aanvraagformulier voor digitaal lesmateriaal. Hiermee wordt het inzichtelijk wie wat aanschaft en of er vooraf aanvullende maatregelen genomen moeten worden, zoals het afsluiten van een verwerkersovereenkomst.

B10: Welke technische maatregelen moet ik geregeld hebben binnen de school?

In overleg met de ICT/netwerk-leverancier worden de volgende maatregelen genomen en periodiek gecontroleerd.

Fysieke beveiliging en continuïteit van ICT

- Persoonsgegevens worden uitsluitend verwerkt in een gesloten, fysiek beveiligde omgeving met bescherming tegen bedreigingen van buitenaf.
- Persoonsgegevens worden uitsluitend verwerkt op apparatuur waarbij maatregelen zijn genomen om de apparatuur fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren.
- Er worden periodiek back-ups gemaakt ten behoeve van de continuïteit van de dienstverlening. Deze back-ups worden vertrouwelijk behandeld, bewaard in een gesloten omgeving en na het verstrijken van de bewaartermijn vernietigd.
- De locaties waar gegevens worden verwerkt worden periodiek getest, onderhouden en periodiek beoordeeld op veiligheidsrisico's

De netwerk-, server- en applicatiebeveiliging

- De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen.
- De omgeving waarbinnen persoonsgegevens worden verwerkt wordt gemonitord.
- Op systemen worden periodiek de laatste (beveiligings)patches en updates geïnstalleerd.
- Penetratietests en vulnerability assessments worden periodiek uitgevoerd.
- Niet (meer) gebruikte informatie wordt verwijderd.
- Op wachtwoorden worden cryptografische maatregelen toegepast om deze gegevens veilig op te slaan.
- Er wordt voor inlogprocessen gebruik gemaakt van versleutelde verbindingen. De uitwisseling van persoonsgegevens aan derden in opdracht van SIO Noord-Holland vindt versleuteld plaats.

Netwerkcomponenten

- De netwerkcomponenten binnen de scholen van SIO Noord-Holland hebben enkel tot doel dat er gebruik kan worden gemaakt van de digitale omgeving van de school, internet, copiers en printers en WIFI. Alle wifi-punten worden automatisch geüpdatet.
- Alle netwerkpunten (switches en routers) worden geüpdatet indien nodig. Alle netwerkcomponenten die password protected ingesteld kunnen worden, zijn beveiligd.

B11: Hoe kan ik aantonen dat ik IBP op orde heb?

Jaarlijks wordt onderstaande (niet uitputtende) controlelijst ingevuld door alle scholen om na te gaan of het handboek is geïmplementeerd, wordt begrepen en nageleefd. De resultaten worden door de FG gerapporteerd aan de bestuurder en Privacy Officer.

	Maatregelen m.b.t. privacy en informatiebeveiliging	**ja/nee**	**Waaruit blijkt dit?**
1	Het **privacyreglement** (zie website) wordt door de schooldirecteur jaarlijks onder de aandacht gebracht van ouders en medewerkers.		
2	Voor de publicatie van **foto- en filmbeelden** en **online diensten** is door de school vooraf **toestemming** vastgelegd.		
3	Met alle leveranciers die namens de school persoonsgegevens verwerken is een **verwerkersovereenkomst** afgesloten.		
4	Voor de uitwisseling van persoonsgegevens met derden, niet zijnde verwerkers, is **toestemming** vastgelegd. Aan het begin van elk schooljaar gaat de school de privacy-voorkeuren van alle ouders na d.m.v. Parro..		
5	De **Procedure melden beveiligingsincidenten en datalekken** is bij de medewerkers bekend. Men weet wat er van hen verwacht wordt.		
6	Toegang tot software en systemen met persoonsgegevens op school worden verleend conform **het vastgestelde toegangsbeleid ParnasSys** (bijlage 1)		
7	De afspraken **over de bewaarplaatsen van gegevens en informatie** (A1) worden nageleefd.		
8	De persoonsgegevens zijn conform de vastgestelde **bewaartermijnen** (B8) opgeschoond.		
9	Er wordt middels o.a. de **gedragscode voor medewerkers** (deel A) en **een protocol ICT en Sociale media voor leerlingen** (bijlage 6) structureel en regelmatig aandacht besteed aan de **voorlichting van medewerkers en leerlingen** ten behoeve van de zorgvuldige verwerking van persoonsgegevens.		
10	Bij **uitdiensttreding** worden alle accounts ingetrokken en apparatuur ingenomen.		
11	Voor alle door de school uitgegeven apparatuur aan medewerkers zijn **gebruikersovereenkomsten** (bijlage 5) afgesloten.		
12	**Fysieke ruimtes** op school met persoonsgegevens van gevoelige aard (op papier of op server) **zijn vergrendeld** tegen onbevoegde toegang.		

Bijlagen

1. Toegangsbeleid ParnasSys

Niet alle medewerkers hebben toegang tot (alle) leerlinggegevens. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien of wijzigen.

Uitgangspunten

- Gegevens van leerlingen en medewerkers worden opgeslagen in de daarvoor aangewezen bewaarplaatsen.
- De afspraken met betrekking tot toegang tot en het verwerken van persoonsgegevens door de verschillende rollen binnen SIO Noord-Holland staan hieronder beschreven in een zogenaamde autorisatiematrix (zie onderstaande tabel A).
- Alle accounts die worden verstrekt dienen te voldoen aan deze autorisatiematrix.
- De directeur van de school is verantwoordelijk voor het verstrekken van de juiste toegang (lees: accounts met de juiste rollen en rechten). De directeur ziet er ook op toe dat de accounts worden ingetrokken na het beëindigen van een arbeids- of samenwerkingscontract of het wijzigen van functies. Daarnaast worden de accounts van systemen met persoonsgegevens periodiek door de applicatiebeheerder gecontroleerd.
- Naast het toepassen van de autorisatiematrix worden de volgende beveiligingsmaatregelen toegepast op systemen waarin persoonsgegevens worden gebruikt:
  - Inloggegevens worden via het e-mailadres van SIO Noord-Holland verstrekt aan de medewerker en nooit gedeeld met anderen.
  - Inloggegevens worden periodiek (minstens 1x per jaar) vernieuwd.
  - Er wordt technisch afgedwongen (waar mogelijk) om sterke wachtwoorden te gebruiken

Toegang tot leerlinggegevens

- Medewerkers hebben alleen toegang tot de leerlinggegevens die noodzakelijk zijn voor de uitoefening van hun functie. Voor leerkrachten betreft dit de gegevens van leerlingen in hun groep(en).
- De accounts worden jaarlijks gecontroleerd op juistheid door of in opdracht van de schooldirecteur.
- De accounts (inclusief rollen en toegangsrechten) worden verstrekt en op inactief gezet door het secretariaat van het CvB in opdracht van de schooldirecteur.

Toegangsbeveiliging

- Inloggegevens van ParnasSys worden via het e-mailadres van SIO Noord-Holland verstrekt aan de medewerker en nooit gedeeld met anderen.
- Computers waar ParnasSys in de internetbrowser is geopend, worden niet onbeheerd achtergelaten.
- De optie “automatisch wachtwoord onthouden” in de internetbrowser wordt niet aangezet voor ParnasSys.

De afspraken met betrekking tot toegang tot en het verwerken van persoonsgegevens door de verschillende organisatierollen binnen SIO Noord-Holland staan hieronder beschreven in een

zogenaamde autorisatiematrix. Alle accounts die worden verstrekt dienen te voldoen aan deze autorisatiematrix.

Indien de organisatierol niet is vermeld in de matrix, dan mag een persoon met deze organisatierol dus ook geen toegang hebben tot ParnasSys. Dat geldt dus in ieder geval voor externen, vrijwilligers (ouders) en reguliere stagiaires, m.u.v. LIO-stagiaires.

De volgende toegangsniveaus worden onderscheiden:

- Alle leerlingen in een specifieke **subgroep** of **groep**
- Alle leerlingen per **school** of op meerdere scholen
- Alle leerlingen binnen de stichting

Tabel A: Autorisatiematrix ParnasSys

Functies/rollen	**Rol in ParnasSys**	**Doelbinding**	**Niveau van toegang:**	**2FA[1]**
Bovenschools				
CvB voorzitter en secretariaat bovenschools	Monitororganisatie Applicatiebeheerder	Sturing, beleid en verantwoording beheer back-up	Stichting	Ja
Stafmedewerker Onderwijskwaliteit	Monitororganisatie stafmedewerker plus Ultimview Applicatiebeheerder Bovenschools	Sturing, beleid, verantwoording	Stichting	Ja
ICT Bovenschools (deze rol is nog niet actief)	Monitororganisatie beheerder Accountbeheerder Applicatiebeheerder Bovenschools	Beheer	Stichting	Ja
School				
Directeur	Applicatiebeheerder	Sturing, Beleid, Verantwoording	School	Ja
Leerkrachten	Leerkracht toegang tot 1 of enkele groepen	Verzorgen onderwijs	School	Nee
Leerlingondersteuner	Leerkracht toegang tot 1 of enkele groepen	Verzorgen onderwijs	School	Nee

[1] *2FA = Two Factor Authentication, oftewel het inloggen met gebruikersnaam, wachtwoord en een tweede middel, zoals een code (token) gegenereerd via app of sleutelhanger.*

Invalleerkracht	Leerkracht beperkt toegang tot relevante groep	Verzorgen onderwijs	Groep	Nee
LIO-stagiaire	Leerkracht toegang tot 1 groep	Verzorgen onderwijs	Groep	Nee
Intern begeleider	Internbegeleider toegang tot alle groepen	Leerlingzorg	School of (sub)-groep	Nee
Administratief medewerker	Administratie Schooladministrateur	Administratie	School	Nee
OSO, Bron	InschrijvenOSO UitschrijvenBRON	Uitwisseling gegevens	School	Nee
Applicatiebeheerder schoolniveau	Applicatiebeheer toegang tot alle groepen	Beheer	School	Ja
Verantwoordelijke absentieregistratie	Verzuimcoördinator	Beheer absentie en verzuim	School	Nee
Ambulant begeleiders / externe hulpverleners	n.t.b.			
Remedial teachers	n.t.b.			
Onderwijsassistenten	n.t.b.			

Medewerkers kunnen via de “Toegangsknop” in ParnasSys, na het invullen van een motivatie die geregistreerd wordt, alsnog op een werkbare wijze tijdelijk toegang krijgen tot andere gegevens, maar dit alles wordt wel goed gelogd en beveiligd. De applicatiebeheerder moet erop toezien dat logbestanden periodiek worden nagegaan en checkt of de redenen die zijn ingevoerd plausibel zijn.

Monitoraanstelling Parnassys

Bij bovenschoolse accounts is het mogelijk om een aanstelling als monitor in te stellen voor je school. Als een gebruiker als monitor is aangesteld op je school, dan wordt deze in ParnasSys niet daadwerkelijk gezien als medewerker van je school. Hij wordt bijvoorbeeld niet meegenomen in medewerkerexports en mailcontacten van de school. Als account- of applicatiebeheerder zie je deze gebruikers wel terug in de medewerkerlijst. Zo is het duidelijk dat voor deze gebruikers toegang is verleend tot je ParnasSys omgeving.

Hoewel een gebruiker met een monitoraanstelling niet wordt gezien als medewerker van een school, is hij wel zichtbaar voor account- en applicatiebeheerders in de schoolomgeving. Zo is voor de school ook duidelijk dat zij toegang hebben tot ParnasSys gegevens.

2. Toelichting voor toestemming gebruik beeldmateriaal

Deze informatie is alleen bedoeld voor de medewerkers van SIO Noord-Holland

Er kunnen goede redenen zijn dat ouders of leerlingen niet willen dat beeldmateriaal van de leerling door de school wordt gepubliceerd. Ouders van een leerling (of de leerling zelf, als deze 16 jaar of ouder is) bepalen zelf of beeldmateriaal van hun kind gepubliceerd mag worden en zo ja waarin en waarvoor. Daarom moet een school altijd toestemming vragen als ze beeldmateriaal van de leerling willen publiceren. Er zijn twee uitzonderingen voor het vragen van toestemming:

1. Er is geen toestemming nodig voor het gebruik van een foto voor identificatiedoeleinden. Het gaat bijvoorbeeld om het plaatsen van een foto op een schoolpas of voor gebruik van een foto in het administratiesysteem.
2. Er is geen toestemming van ouders nodig voor het gebruik van beeldmateriaal in de klas en les voor onderwijskundige doeleinden, mits die beelden niet gepubliceerd worden (en alleen maar in de les worden gebruikt). Denk bijvoorbeeld aan het maken van een versierd fotolijstje met een foto van de leerling als cadeau voor Moederdag, of een tekenopdracht om een zelfportret te maken aan de hand van een foto.

De wetgever eist dat een ouder een goed geïnformeerde beslissing kan nemen, die ook specifiek is. Het vragen van toestemming ‘voor gebruik van foto’s door de school’ is dat zeker niet. Als school mag je het dus niet zo formuleren: ‘als u niet wilt dat we foto’s van uw kind gebruiken, moet u dat maar zeggen’. Dit is een ‘opt-out’, en dit is in strijd met de wet. In het toestemmingsformulier wordt dan ook duidelijk aangegeven waar beeldmateriaal voor gebruikt mag worden en met welk doel.

Klassenfoto

Deze foto is een leuke herinnering voor later, en het is traditie dat deze foto jaarlijks wordt gemaakt. Maar er kunnen goede redenen zijn dat een ouder niet wil dat zijn/haar kind op de klassenfoto wordt gezet, of dat de foto met zijn/haar kind bij andere ouders/familie van klasgenoten terechtkomt. Vraag dus altijd toestemming voor het maken van de klassenfoto. Heb je van een leerling geen toestemming voor het maken van de klassenfoto? Dan gaat hij/zij niet op de klassenfoto!

Foto’s maken door ouders op school

Het kan voorkomen dat ouders het vervelend vinden dat andere ouders foto’s maken van hun kinderen. Meestal overleggen deze ouders samen over het maken en gebruik van die foto’s. Soms komen ouders samen er niet uit en dan wordt de school gevraagd om iets te regelen. De school wil voor álle kinderen een veilige omgeving zijn en niet een plek waar kinderen (en hun ouders) bang hoeven te zijn steeds te worden gefotografeerd. Het maken van foto’s en video’s op school kan moeilijk worden verboden, maar kan wel aan banden worden gelegd. Door bijvoorbeeld verwachtingen uit te spreken naar ouders over fotograferen tijdens een schoolactiviteit, of door ouders in de nieuwsbrief te vragen terughoudend te zijn met het maken en publiceren van foto’s. Mocht dat niet het gewenste effect hebben, dan kan de school regels voor het maken van foto’s op school vastleggen. Een schoolgebouw is niet zomaar een openbare plaats waar iedereen toegang toe heeft. De school kan aan het verlenen van toegang dus voorwaarden stellen zoals de (extreme) regel dat fotograferen van leerlingen tijdens de les of in de klas alleen is toegestaan door docenten.

N.B. Als er beeldmateriaal op het beveiligde deel van de website door ouders gekopieerd wordt en vervolgens gedeeld via sociale media is dat niet meer de verantwoordelijkheid van de school. De

school doet er wel goed aan om dit bij ouders onder de aandacht te brengen en hen te wijzen op hun verantwoordelijkheid hierin.

Toestemming geven door één of twee ouders

Het is de vraag of de toestemmingverklaring door één of beide ouders moet worden ondertekend. Als leerlingen jonger zijn dan 16 beslissen de wettelijk vertegenwoordigers (de ouders) over de privacy van hun kinderen. De wet gaat ervan uit dat je als school mag vertrouwen op de mededelingen van één ouder. Als dat vertrouwen terecht is, dan is de andere ouder ook gebonden aan die mededeling. Bij het ondertekenen van de toestemmingsverklaring, mag de school dus vertrouwen op de toestemming als één ouder die geeft. Alleen als de school weet dat de andere ouder (die niet getekend heeft) tegen de toestemming is, mag de school niet uitgaan van die ene ondertekening. Dan moet de school van beide ouders toestemming hebben. Vooral bij gescheiden ouders kan het verstandig zijn om beide ouders toestemming te vragen. Voor het intrekken van toestemming is de mededeling van één ouder ook voldoende. Bij twijfel is het beter om te vertrouwen op twee handtekeningen, of om de foto dan maar niet te gebruiken.

Voorbeeldtekst overige toestemming

[LOGO Stichting]

[Plaats], [maand] [jaar]

In het kader van privacywetgeving, willen wij u toestemming vragen voor het delen van de volgende persoonsgegevens. U mag natuurlijk altijd terugkomen op de door u gegeven toestemming. Ook mag u op een later moment alsnog toestemming geven. Neem hiervoor contact op met <naam directeur>, via <mailadres directeur>.

Hierbij verklaart ondergetekende, ouders/verzorger van ……, dat:

Zijn/haar [omschrijving persoonsgegevens] WEL/ NIET * gedeeld mag worden met andere ouders (* streep door wat niet van toepassing is)

Ouder/verzorger 1 Ouder/verzorger 2

Naam:

Datum:

Plaats:

Handtekening

3. Geheimhoudingsverklaring

[De heer/mevrouw] [naam], hierna 'Gebruiker', werkzaam op basis van een overeenkomst van opdracht voor Stichting Islamitisch Onderwijs Noord-Holland, gevestigd te Amsterdam.

Verklaart zich akkoord met het volgende:

1. Gebruiker (niet zijnde een personeelslid in dienst van SIO Noord-Holland) heeft uit hoofde van zijn/haar opdracht toegang tot persoonsgegevens van leerlingen en/of personeel. Gebruiker heeft kennisgenomen van het Privacyreglement en het Handboek Privacy van SIO Noord-Holland en de daarin opgenomen voorschriften die gelden bij het verwerken van persoonsgegevens waartoe hij toegang heeft.
2. Het is Gebruiker zowel gedurende als na afloop van de overeenkomst van opdracht met SIO Noord-Holland/zijn werkzaamheden voor SIO Noord-Holland verboden om - ongeacht de wijze waarop en de redenen waarom de overeenkomst/de werkzaamheden tot een einde is/zijn gekomen - op enigerlei wijze aan derden, direct of indirect, in welke vorm en op welke wijze dan ook enige mededeling te doen van of aangaande gegevens betreffende de leerlingen en personeel, waarvan Gebruiker in het kader van de uitoefening van zijn werkzaamheden voor SIO Noord-Holland kennis heeft genomen.
3. Deze persoonsgegevens zijn privacygevoelig en mogen uitsluitend worden verwerkt voor het doel waarvoor ze zijn verkregen. Gebruiker zal zich bij zijn werkzaamheden ervan vergewissen dat gegevens van leerlingen en personeel uitsluitend worden gedeeld conform het bepaalde in het Privacyreglement.
4. Dat de Gebruiker uiterste zorg besteedt aan een deugdelijke en veilige opslag van de informatie en/of persoonsgegeven, ter voorkoming van verlies en/of enige vorm van onrechtmatige verwerking, en hiertoe de richtlijnen en instructies opvolgt die SIO Noord-Holland verstrekt en voorschrijft. De gebruiker zal geen kopieën van de informatie bewaren.
5. Indien Gebruiker een (mogelijke) inbreuk op de beveiliging signaleert waarbij (mogelijk) persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, meldt de Gebruiker dit per omgaande aan privacy@sionoord-holland.nl

[Plaats] [datum]:

_____

[Naam]

4. Aanvraagformulier digitaal lesmateriaal

Datum aanvraag: Naam applicatie:

Gegevens aanvrager	Locatie *		
	Naam aanvrager *		
	Sectie/vak *		
Gegevens leverancier	Naam *		
	Contactpersoon		
	Adres		
	Vestigingsplaats		
	Telefoon		
	E-mail/ Website *		
Gegevens digitaal lesmateriaal	Naam softwarepakket en de versie *		
	Omschrijving (Wat kan het pakket)	□ aanvulling op methode	
	Eenmalige aanschafkosten*	€	
	Jaarlijkse licentiekosten *	€	
	Eventuele overige kosten *	€	
	Freeware/ demo of evaluatiesoftware *	□ Ja	□ Nee
	Internetapplicatie (Webbased) *	□ Ja	□ Nee
	Moeten leerlingen zelf inloggen* Zo ja: waarmee/hoe*	□ Ja	□ Nee
	Aantal gebruikers waarvoor licentie nodig is *		
	Software reeds geleverd/ beschikbaar *	□ Ja	□ Nee
Criteria	Software onderwijskundig geschikt. Sectie akkoord*	□ Ja	□ Nee
	Gecontroleerd op aanwezigheid van vergelijkbare software binnen de organisatie *	□ Ja	□ Nee
Akkoord Handtekeningen lijst		Schooldirecteur	
	Naam		
	Handtekening		

*verplicht

5. Model Gebruikersovereenkomst voor device in bruikleen bij medewerkers

[Onderwijsinstelling] te [Plaats], in deze vertegenwoordigt door [Naam], [functie], hierna te noemen werkgever en [Naam medewerk(st)er], personeelsnummer [nummer], werkzaam als [functie] bij [Onderwijsinstelling], hierna te noemen werknemer:

verklaren dat zij een gebruikersovereenkomst voor bedrijfsmiddelen ICT, verder te noemen "apparatuur", voor [duur] zijn aangegaan. De navolgende voorwaarden zijn op deze overeenkomst van toepassing:

- Werkgever verstrekt aan werknemer de apparatuur ten behoeve van de uitoefening van de werkzaamheden van de dienstbetrekking.
- De apparatuur is eigendom van werkgever en wordt in bruikleen gegeven aan werknemer.
- Deze overeenkomst bepaalt de nadere gebruiksvoorwaarden waaronder de werknemer de apparatuur kan gebruiken.
- Door ondertekening aanvaardt de werknemer alle voorwaarden van deze overeenkomst.

Aard en uitvoering

Het type apparatuur en/of het abonnement wordt door werkgever vastgesteld en aangeschaft.

Rechten en plichten werknemer

a. Werknemer verklaart de apparatuur in goede staat te hebben ontvangen en zal deze niet aan derden ter beschikking stellen, verpanden of op enigerlei andere wijze vervreemden.
b. Werknemer is verantwoordelijk voor het in goede en representatieve staat houden van de apparatuur.
c. Tijdens een ziekteperiode van de werknemer van 6 weken of langer, moet de apparatuur ingeleverd worden bij de werkgever, tenzij hierover afspraken worden gemaakt met de leidinggevende.
d. Het is werknemer niet toegestaan zonder toestemming van de direct leidinggevende de apparatuur tijdens verlof mee te nemen naar het buitenland. Ook is bellen naar en vanuit het buitenland niet toegestaan.
e. Het is werknemer niet toegestaan zonder toestemming van de werkgever wijzigingen in de configuratie van de apparatuur aan te brengen.
f. Het is werknemer verboden de apparatuur te gebruiken voor activiteiten die in strijd zijn met de bedrijfsdoelstellingen of het aanzien van de werkgever schade (kunnen) berokkenen, dan wel de grenzen van betamelijkheid en fatsoen overschrijden.
g. Werknemer is op de hoogte dat werkgever het gebruik van de apparatuur door de werknemer controleert op het zakelijk gebruik van de apparatuur. Door ondertekening van deze overeenkomst stemt de werknemer in met deze controle. Tevens verklaart werknemer zich bereid alle medewerking te verlenen die noodzakelijk is om zakelijk gebruik te kunnen onderbouwen.
h. Werknemer verklaart zich akkoord dat indien werknemer heeft gehandeld in strijd met de bepalingen van deze gebruikersovereenkomst, eventueel daaruit voortvloeiende kosten zullen worden verhaald op werknemer.

Gebruik apparatuur

De werknemer wordt voor de uitoefening van zijn dienstbetrekking de apparatuur ter beschikking gesteld die werknemer voor minder dan € [bedrag] per jaar voor privédoeleinden gebruikt. Bij het belastbare loon van de werknemer wordt maandelijks een bedrag van € [bedrag] geteld voor het privégebruik van de mobiele telefoon.

Diefstal en beschadiging

a. Werknemer dient afdoende beschermingsmaatregelen te treffen, zoals periodiek wijzigen van wachtwoorden en dergelijke, ter bescherming van gegevens op de apparatuur.
b. Werknemer dient alle zorgvuldigheid in acht te nemen ter voorkoming van beschadiging, diefstal of verlies van de apparatuur.
c. In geval van schade aan of diefstal van de apparatuur is werknemer verplicht dit zo spoedig mogelijk, doch uiterlijk binnen 24 uur bij werkgever te melden. Als contractant draagt werkgever het risico voor misbruik na diefstal, mits aan het hiervoor gestelde is voldaan.
d. Werknemer kan aansprakelijk worden gesteld voor verlies van of schade aan de apparatuur ontstaan door verwijtbare nalatigheid of onachtzaamheid. Kosten voor herstel of vervanging kunnen in dat geval worden ingehouden op het salaris van medewerker.

Termijn van gebruik

a. Werknemer dient de apparatuur binnen de afgesproken bruikleentermijn dan wel bij beëindiging van het dienstverband of functieverandering op eerste verzoek in volledige staat te retourneren. Bij verzuim hiertoe, verbindt werknemer zich tot betaling van de rest(boek)waarde van de apparatuur aan werkgever.
b. Indien werknemer na het einde van de bruikleenovereenkomst of na opzegging hiervan door werkgever niet onmiddellijk voldoet aan een verzoek van werkgever tot teruggave van de apparatuur, verbeurt werknemer een boete van € [bedrag] voor iedere dag, dat werknemer, na bij aangetekende brief door werkgever vermaand te zijn, aan zijn verplichtingen niet voldoet.
c. Indien één van de genoemde gevallen in deze gebruikersovereenkomst zich voordoet, is werkgever bevoegd een geschil betreffende de teruggave van de apparatuur aan het oordeel van de President van de arrondissementsrechtbank te [Plaats], rechtsprekende in kort geding, te onderwerpen.
d. Door ondertekening van deze overeenkomst verklaart werknemer dat hij gevolgen van deze overeenkomst heeft begrepen en zich daarmee akkoord verklaart.

Aldus verklaard, opgemaakt in tweevoud en ondertekend te [Plaats],

[Naam onderwijsinstelling]

....

Naam: Naam:

Datum: Datum:

6. Model Gebruikersovereenkomst voor device in bruikleen bij leerlingen

De gebruiker en/of diens wettelijke vertegenwoordiger is bekend met de inhoud van de bruikleenovereenkomst en verklaart zich hiermee akkoord. Het device wordt in bruikleen aan de gebruiker verstrekt en blijft eigendom van SIO Noord-Holland. Het beschikbaar gestelde device betreft een:

[….]

Artikel 1

Algemene uitgangspunten

1.1. De gebruiker is zich ervan bewust dat het device, dat hij/zij in bruikleen krijgt van SIO Noord-Holland, volledig eigendom is en blijft van SIO Noord-Holland.

1.2. Aan het einde van de looptijd zal op verzoek van SIO Noord-Holland het device uiterlijk één dag na het einde van de looptijd aan school worden geretourneerd.

1.3. De gebruiker dient zelf te zorgen dat het device elke lesdag opgeladen is en klaar om te gebruiken. 1.4. Het in bruikleen krijgen van het device door de gebruiker van SIO Noord-Holland heeft een persoonlijk karakter en is op geen enkele wijze aan derden overdraagbaar onder algemene of bijzondere titel.

1.5. Bij schade, diefstal of verlies stelt SIO Noord-Holland tijdelijk een vervangend device beschikbaar.
1.6. De device mag alleen bij de leerling thuis gebruikt worden en nergens anders mee naar toe worden genomen.

Artikel 2

Gebruik (rechten en plichten van de gebruiker)

2.1. Verlies of schade van het device, de adapter en oplaadkabel valt onder het eigen risico en is derhalve voor rekening gebruiker of diens wettelijke vertegenwoordiger.

2.2. De gebruiker is verplicht de nodige zorg te betrachten bij het gebruik, zodanig dat het naar behoren functioneren van het device gewaarborgd blijft.

2.3. De gebruiker zal maatregelen treffen zodat risico’s voor het beschadigen tot een minimum beperkt blijven.

2.4. De kosten van schade of verlies van het device, waarbij is vast komen te staan dat deze ontstaan is door opzet of merkelijke schuld van de gebruiker, komen onder alle omstandigheden voor rekening van de gebruiker.

2.5. Privégebruik is binnen de grenzen van het redelijke toegestaan, maar mag de functionaliteit van het device ten behoeve van het schoolwerk niet beïnvloeden.

2.6. Het is, behoudens uitdrukkelijke schriftelijke toestemming van SIO Noord-Holland, aan de gebruiker verboden om het device, aan een ander in gebruik af te staan of aan een ander te verhuren.

2.7. De gebruiker blijft te allen tijde verantwoordelijk voor het beheer van data t.b.v. privédoeleinden op het device.

2.8. Eventueel aan de gebruiker uitgereikte wachtwoorden en/of pincodes, zijn strikt persoonlijk en dient de gebruiker strikt geheim te houden.

2.9. Bij schade aan het device, dient de gebruiker dit onmiddellijk schriftelijk (via email) aan de SIO Noord-Holland school te melden.

2.10. Bij verlies of diefstal van het device dient de gebruiker dit onmiddellijk schriftelijk (via email) aan de SIO Noord-Holland school te melden en hiervan binnen 24 uur aangifte te doen bij de politie. Een kopie van de aangifte dient te worden verstuurd naar school.

Artikel 3

Gebruiksvoorwaarden van de Device SIO Noord-Holland

3.1. Het is de gebruiker niet toegestaan om instellingen, die door SIO Noord-Holland zijn ingesteld, op het device te wijzigen.

3.2. Het is de gebruiker niet toegestaan om de op het device aangebrachte software, geheel of gedeeltelijk, dan wel tijdelijk ofwel permanent onklaar te maken.

3.3. SIO Noord-Holland kan niet worden aangesproken op het verlies van data als de gebruiker handelingen heeft verricht, die niet toegestaan zijn op grond van de gebruiksvoorwaarden in dit artikel, en op de hieruit voortvloeiende, door SIO Noord-Holland uitgevoerde herstelwerkzaamheden.

3.4. Alleen met een door de verzekeringsmaatschappij goedgekeurde hoes is het device verzekerd.

3.5. SIO Noord-Holland is bevoegd de overeenkomst tussentijds en zonder enige opzegtermijn op te zeggen en van gebruiker de onmiddellijke teruggave van het device te verlangen indien gebruiker het device verwaarloost, misbruikt, voor een ander doel gebruikt dan waarvoor deze bestemd is of gebruiker op enigerlei andere wijze in strijd handelt met de bepalingen van deze overeenkomst.

Dit gebruiksreglement is door de bestuurder van SIO Noord-Holland vastgesteld. In alle gevallen waarin deze regeling niet voorziet, beslist de bestuurder.

Aldus verklaard, opgemaakt in tweevoud en ondertekend te [Plaats],

[Naam onderwijsinstelling]

....

Naam: Naam:

Datum: Datum:

7. Voorbeeldprotocol ICT en Sociale media voor leerlingen

N.B. Dit is hetzelfde voorbeeldprotocol als in het Bovenschools Veiligheidsplan.

A. Internet en e-mail

We vinden het van groot belang dat je als leerling zo veilig mogelijk online kan werken. Om hiervoor te zorgen, zijn de volgende gedragsregels van belang:

1. Ik gebruik het internet met toestemming om het COOL-portaal te openen.
2. Ik vraag toestemming van mijn meester of juf, als ik…
    a. Een online game wil spelen
    b. Persoonlijke gegevens (naam, adres en je telefoonnummer) moet invullen op een website
    c. Bestanden wil downloaden of delen
    d. Een e-mail wil versturen
3. Ik deel geen wachtwoorden met anderen.
4. Ik ga voorzichtig om met mails die ik niet vertrouw of waarvan ik de afzender niet ken. Bij twijfel klik ik geen links aan.
5. Ik vertel direct aan mijn meester of juf als ik informatie tegenkom die ik niet prettig vind of waarvan ik weet dat dat niet hoort.
6. Ik weet bij welke instanties/personen ik op school en buiten school terecht kan als ik iets onprettigs heb meegemaakt op het internet waarbij ik me niet veilig voel.
7. Ik bekijk informatie op internet kritisch en kan beoordelen of het echt of nep is.
8. Ik ken de gevolgen van het delen van informatie die niet echt is.

B. Sociale media

Binnen de school gelden de volgende gedragsregels om te zorgen dat de mogelijkheden van sociale media worden gebruikt zonder andere personen of de school te schaden:

9. Ik plaats geen foto’s of verhalen over een ander (leerling, juf of meester, school, ouders of anderen van buiten de school) op sociale media als een ander dit niet goed vindt.
10. Ik plaats geen kwetsende foto’s, verhalen of opmerkingen op sociale media. Ook gebruik ik geen grove taal.
11. Ik doe niet mee aan pesten via Whatsapp of via welke sociale media dan ook, Als ik nare berichten ontvang van iemand, dan vertel ik dit op school of thuis.
12. Als ik iemand niet begrijp via de Whatsapp of andere berichten, dan vraag ik dit rechtstreeks aan diegene.
13. Ik ga zorgvuldig om met mijn eigen identiteit. Ik besef dat ik altijd terug te vinden ben op internet.

C. ICT-apparatuur

Je dient voorzichtig met de ICT-apparatuur op school (laptop, tablet, digibord, scanner, etc.) om te gaan. De volgende gedragsregels zijn daarom van belang:

14. Ik gebruik alleen ICT-apparatuur en software waar ik toestemming voor heb gekregen van de meester of juf. Dat geldt ook voor meegebracht smartphones, etc.
15. Ik ga voorzichtig om met de dure ICT-apparatuur van de school die ik mag gebruiken.
16. Ik gebruik geen meegebrachte USB-sticks van thuis in ICT-apparatuur van de school

8. Tekst voor op de website en/of in de schoolgids

Privacy en leerlinggegevens

De gegevens die over leerlingen gaan, noemen we persoonsgegevens. In het privacyreglement [link] van het bestuur is beschreven hoe de school omgaat met persoonsgegevens, en wat de rechten zijn van ouders en leerlingen. Dit reglement is met instemming van de GMR vastgesteld.

Wij maken alleen gebruik van persoonsgegevens als dat nodig is voor het leren en begeleiden van onze leerlingen, en voor de organisatie die daarvoor nodig is. De meeste gegevens ontvangen wij van ouders bij de inschrijving op onze school. Daarnaast registreren leerkrachten en ondersteunend personeel gegevens over leerlingen, bijvoorbeeld cijfers en vorderingen. Soms worden er bijzondere persoonsgegevens geregistreerd als dat nodig is voor de juiste begeleiding van een leerling, zoals medische gegevens (denk aan dyslexie of ADHD). De leerlinggegevens worden opgeslagen in ons (digitale) administratiesysteem ParnasSys. Dit programma is beveiligd en toegang tot die gegevens is beperkt tot medewerkers van de stichting die de gegevens strikt noodzakelijk nodig hebben voor de uitvoering van hun werkzaamheden.

Tijdens de lessen maken wij gebruik van digitale leermiddelen. Hiervoor wordt een beperkte set met persoonsgegevens uitgewisseld met leveranciers om bijvoorbeeld een leerling te identificeren als die inlogt.

Wij hebben met leveranciers duidelijke afspraken gemaakt over de gegevens die ze van ons krijgen. De leverancier mag de leerlinggegevens alleen gebruiken als wij daar toestemming voor geven. Een lijst van de leveranciers waar de school afspraken mee heeft gemaakt, is op te vragen bij de school.

Daarnaast kan het nodig zijn dat wij gegevens uitwisselen met andere externe partijen, denk aan zorginstanties. Deze zijn vermeld in het privacyreglement. Als voor de uitwisseling geen wettelijke verplichting bestaat, dan vragen wij u vooraf toestemming om met deze partijen gegevens te mogen uitwisselen.

Bij de inschrijving van uw kind(eren) vragen wij u om toestemming voor het gebruik van foto- en videomateriaal, het delen van uw contactgegevens met andere ouders en het gebruik van sociale media door uw kind(eren). U hebt te allen tijde het recht om deze toestemming te wijzigen. U kunt dit kenbaar maken via een mail aan de directeur en via de app Parro.

De school vraagt ouders nadrukkelijk om terughoudend te zijn met het maken van foto’s en video’s binnen de school. Het is ouders niet toegestaan om foto’s/video’s die gemaakt zijn op school te delen via sociale media of te gebruiken voor commerciële doeleinden.

Als u vragen of verzoeken heeft op het gebied van privacy kunt u terecht bij de schooldirecteur of via privacy@sionoord-holland.nl. SIO Noord-Holland heeft ook een Functionaris Gegevensbescherming om toezicht te houden op de bescherming van privacy en persoonsgegevens: dhr. Haci Karacaer. U kunt hem met eventuele vragen benaderen via fg@sionoord-holland.nl

9. Informatiebeveiliging en Privacybescherming (IBP)

1 Verantwoording en richtlijnen

1.1 Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid en de daaraan verbonden afspraken en procedures is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

1.2 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een aantal samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.

Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten volledig, juist en actueel zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

1.3 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:

Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

1.4 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: Informatiebeveiliging en privacy (IBP). Dit beleid, verder te benoemen

als IBP-beleid, vormt de basis om IBP binnen het bestuur van SIO Noord-Holland te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

2 Doel en reikwijdte

2.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen van wie het bestuur van SIO Noord-Holland persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het IBP-beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en het bestuur van SIO Noord-Holland voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het IBP-beleid binnen SIO Noord-Holland geldt voor alle betrokkenen, te weten: medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/ outsourcing).
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het bestuur van SIO Noord-Holland. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of sociale media.) Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van het bestuur van SIO Noord-Holland evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die handmatig in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- IBP-beleid heeft binnen het bestuur van SIO Noord-Holland raakvlakken met:
  - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
  - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
  - IT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT vanuit Cloudwise en (digitale) leermiddelen
  - Medezeggenschap ouders/verzorgers en medewerkers

2.3 Concretisering van het beleid – Hoe doen we dat?

Het bestuur van SIO Noord-Holland hanteert de volgende taken om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het **Bestuur** van SIO Noord-Holland neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld is. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
2. Het bestuur van SIO Noord-Holland voldoet aan alle **relevante wet- en regelgeving**.
3. Bij SIO Noord-Holland is de verwerking van persoonsgegevens altijd gekoppeld aan een **specifiek doel** en gebaseerd op één van de **wettelijke grondslagen**. Een goede balans tussen het belang van het bestuur van SIO Noord-Holland om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen op elk moment hun toestemming herzien.
4. SIO Noord-Holland zal alle **betrokkenen helder en actief informeren** over de verwerking van de persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering van hun persoonsgegevens.
5. SIO Noord-Holland legt alle **verwerkingen van persoonsgegevens** vast in een register voor verwerkingsactiviteiten (het **dataregister**), en zal deze up-to-date houden. Het bestuur van SIO Noord-Holland voldoet hiermee aan de documentatieplicht, zoals benoemd in de AVG.
6. Binnen het bestuur van SIO Noord-Holland is het **veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen**. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
7. Het bestuur van SIO Noord-Holland is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het **eigendom** (auteursrecht) **toebehoort aan derden**. Medewerkers en leerlingen mogen geen content downloaden waar intellectuele eigendomsrechten op rusten als er geen licentie door SIO Noord-Holland is afgesloten. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. SIO Noord-Holland **classificeert informatie en informatiesystemen**. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken, de benodigde investeringen en de te nemen maatregelen.
9. SIO Noord-Holland sluit met **alle leveranciers van digitale onderwijsmiddelen** (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken.
10. Het bestuur van SIO Noord-Holland verwacht van **alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen** met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. SIO Noord-Holland heeft hiervoor afspraken in de **gedragscode veilig gebruik ICT-middelen en persoonsgegevens** geformuleerd, vastgesteld en geïmplementeerd. Hierin staan afspraken over onder andere het computergebruik, applicatiegebruik, opslag (persoons)gegevens, communicatie, digitale veiligheid en het melden van beveiligingsincidenten en datalekken.

11. **Informatiebeveiliging en privacy is bij SIO Noord-Holland een continu kwaliteitsproces**, waarbij regelmatig (minimaal jaarlijks) op basis van evaluatie, audit of zelf-assessment wordt gekeken of aanpassing gewenst dan wel noodzakelijk is.
12. SIO Noord-Holland kijkt bij **wijzigingen** in de infrastructuur of de **aanschaf van nieuwe (informatie)systemen** vóóraf naar de impact hiervan op de informatiebeveiliging en privacy. Indien noodzakelijk wordt er een Data Protectie Impact Assessment (DPIA). De uitkomst van de DPIA bepaalt de te nemen aanvullende maatregelen.
13. SIO Noord-Holland neemt **passende organisatorische en/of technische (beveiligings-)maatregelen** om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren. Afspraken rondom de technische maatregelen zijn vastgelegd in de verwerkersovereenkomst met Cloudwise.
14. SIO Noord-Holland zal alle **beveiligingsincidenten vastleggen en datalekken** volgens een vast protocol afhandelen en – indien nodig - melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.
15. SIO Noord-Holland gaat ten aanzien van informatiebeveiliging (**autorisatie en authenticatie**) ervan uit dat "Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten" en niet van het uitgangspunt "Alles is in principe toegelaten tenzij het uitdrukkelijk is verboden"

3. Uitvoering van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten.

3.1 Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Het internationale normenkader voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

SIO Noord-Holland hanteert de laatste versie van het hiervan afgeleide Toetsingskader Informatiebeveiliging en Privacy dat ontwikkeld is door Privacy op School.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

3.2 Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen met betrekking tot de verwerking van persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de volgende **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens:

1. Doelbepaling en doelbinding: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld, inclusief de bewaartermijnen. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. Grondslag: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen (toestemming, uitvoering van een overeenkomst, wettelijke verplichting, vitaal belang, algemeen belang en gerechtvaardigd belang)
3. Dataminimalisatie: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. Transparantie: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante manier verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Het geven van deze informatie vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op inzage, verbetering, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit, afscherming en profilering van

hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

5. Data-integriteit: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens volledig, juist en actueel zijn.

3.3 Ondersteunende beleidsafspraken en procedures

Diverse aanvullende beleidsafspraken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up to-date gehouden in een register voor verwerkingsactiviteiten. Hiervoor worden het Dataregister voor Leerlingen, Medewerkers en Relaties gebruikt.

3.4 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de directeuren, bestuurders en de FG met het algemeen bestuur als eindverantwoordelijke.

3.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitscriteria die van belang zijn.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy. Op basis van de uitkomst van een centraal ingeregelde DPIA (Data Protection Impact Assessment) worden vervolgens passende maatregelen genomen. Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

3.6 Incidenten en datalekken

Alle medewerkers en leerlingen, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in de Procedure beveiligingsincidenten en datalekken. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings-)incidenten worden vastgelegd in een incidentenregister. Het melden van (beveiligings-)incidenten kan intern via privacy@SIOnoord-holland.nl. De bestuurder bekijkt of de meldingen moeten worden doorgezet naar fg@SIOnoord-holland.nl.

3.7 Planning en controle

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten SIO Noord-Holland maken het noodzakelijk om periodiek te controleren of het beleid nog voldoet aan de eisen. Dit IBP-beleid wordt minimaal elke twee jaar getoetst en indien nodig door het bestuur bijgesteld. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- De actuele geïnventariseerde risico's;
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

SIO Noord-Holland kent tevens een jaarlijkse verbetercyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid (IBP-beleid) wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving enz. meegenomen. Het resultaat hiervan wordt vastgelegd in een nieuwe versie van het handboek.

3.8 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid, richtlijnen en procedures. Naleving van het IBP-beleid is een primaire verantwoordelijkheid van alle medewerkers binnen SIO Noord-Holland. Daarnaast neemt de directeur de verantwoordelijkheid om medewerkers aan te spreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, d.m.v. een gedragscode, periodieke bewustwordingscampagnes, et cetera.

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG is aangesteld door de bestuurder, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan het bestuur van SIO Noord-Holland de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

3.9 Logging en monitoring

Logging en monitoring door de IT-afdeling van Cloudwise zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens worden vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk. SIO Noord-Holland zal deze logging regelmatig (laten) beoordelen.

4 Governance – Wie doet wat?

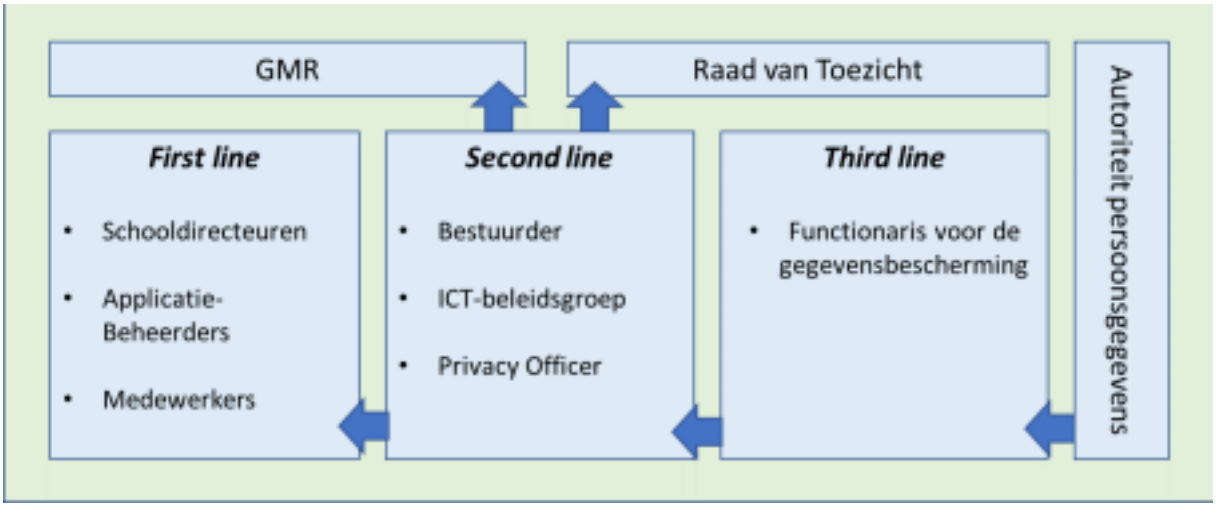
4.1 Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Voor een optimaal IBP-beleid moet dit goed ingeregeld zijn, met andere woorden de governance moet op orde zijn.

Het bestuur van SIO Noord-Holland hanteert het 'three lines of defence model'. De eerste lijn binnen dit model is cruciaal. Hierin is vastgelegd dat directeuren toezien op het verantwoord omgaan met persoonsgegevens. Directeuren zien erop toe dat al hun teamleden handelen volgens het vastgestelde Handboek Privacy en de daarbij behorende afspraken en procedures.

De tweede lijn ondersteunt de 1e lijn en adviseert, coördineert en bewaakt of de directies hun verantwoordelijkheid daadwerkelijk nemen. Daarnaast zijn bepaalde beleidsvoorbereidende taken en het organiseren van integrale risicoanalyses taken van de tweede lijn. De derde lijn controleert en beoordeelt de effectieve werking van de tweede lijn en eerste lijn en geeft daarover een objectief, onafhankelijk oordeel met mogelijkheden tot verbetering. Het dagelijks bestuur is als verwerkingsverantwoordelijke eindverantwoordelijk voor het beschermen van de privacy van alle betrokkenen.

Schematisch wordt dit als volgt weergegeven.



4.2 De first line of defence is primair verantwoordelijk

Hieronder vallen de directies, applicatiebeheer en de verschillende medewerkers.

De eerste lijn bewaakt het IBP-beleid binnen hun eigen organisatorische onderdeel. Zij vormen de first line of defence als het gaat om de bescherming van persoonsgegevens. Zij voeren de daarbij behorende operationele taken uit op basis van het door de tweede lijn ontwikkelde beleid en daarbij behorende richtlijnen en procedures, zoals:

- Toetsen dat er geen andere verwerkingen plaatsvinden dan die zijn vastgelegd in de registers voor verwerkingen; de dataregisters voor leerlingen, medewerkers en relaties;

- Toetsen op het afsluiten van verwerkersovereenkomsten of privacyregelingen als persoonsgegevens worden overgedragen aan externe partijen;
- Signaleren en beoordelen van incidenten waarbij persoonsgegevens betrokken zijn en het intern melden daarvan als het vermoeden bestaat dat het gaat om een datalek.

Directeuren voeren bovendien de volgende operationele taken uit:

- Nagaan of medewerkers voldoende voorgelicht zijn over de AVG wetgeving.
- Vastleggen van de extra taken en rollen van medewerkers en de daarbij behorende rechten binnen de bijbehorende systemen, zoals ParnasSys.

4.3 De second line of defence: bestuurder en de Privacy Officer van SIO Noord-Holland

De bestuurder en de Privacy Officer werken samen binnen de second line of defence als het gaat om de bescherming van persoonsgegevens. De tweede lijn

- Ontwikkelt waar nodig beleid op het gebied van informatiebeveiliging en privacy. Het dagelijks Bestuur stelt het voorgenomen beleid vast;
- Monitort en evalueert de toepassing en naleving van het informatiebeveiligings- en privacybeleid en de daaraan gekoppelde afspraken en procedures;
- Adviseert over informatiebeveiliging en privacybescherming;
- Ondersteunt de eerste lijn bij het identificeren en bewaken van risico's.

4.4 De third line of defence: Functionaris voor Gegevensbescherming als interne auditor

SIO Noord-Holland heeft een externe toezichthouder op de verwerking van persoonsgegevens aangesteld, de functionaris voor gegevensbescherming (FG) genoemd. De FG zal door SIO Noord-Holland tijdig worden betrokken bij alle aangelegenheden waar persoonsgegevens bij komen kijken.

De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. SIO Noord-Holland heeft de FG aangemeld bij de Autoriteit Persoonsgegevens.

De taken van de FG houden in:

- Het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG;
- Het toezien op de naleving van de AVG en andere relevante privacywetgeving;
- Het toezien op de naleving van dit IBP-beleid van het bestuur van SIO Noord-Holland;
- Het toezien op een Data Protection Impact Assessment (DPIA);
- Het behandelen van klachten over de toepassing van het privacyreglement;
- Het fungeren als eerste aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

In bijlage 1 zijn alle taken en verantwoordelijkheden uitgewerkt.

4.5 Implementatie beleid

Het Bestuur van SIO Noord-Holland is verantwoordelijk voor verwerkingen van persoonsgegevens waarvoor zij het doel en de middelen vaststelt. Als verwerkingsverantwoordelijke in de zin van de AVG houdt de verantwoordelijkheid kort samengevat in dat:

- persoonsgegevens worden alleen verwerkt in overeenstemming met de vastgestelde doelen voor de verwerking. Deze doelen moeten gerechtvaardigd zijn en de verwerking moet zorgvuldig gebeuren;
- hierover aantoonbaar verantwoording kan worden afgelegd aan de Autoriteit Persoonsgegevens.

De feitelijke verwerking van persoonsgegevens wordt op verschillende lagen binnen het bestuur van SIO Noord-Holland uitgevoerd. Er is een onderscheid tussen centrale verwerkingen, waarvoor het bestuurskantoor verantwoordelijk is en decentrale verwerkingen, waarvoor organisatieonderdelen of locaties verantwoordelijk zijn. Echter, in alle gevallen behoudt het bestuur als verantwoordelijke in de zin van de AVG de eindverantwoordelijkheid voor de zorgvuldige verwerking van persoonsgegevens binnen de gehele organisatie.

4.6 Controle en naleving

AVG audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert met de tweede lijn de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens. Met de AVG audit kan aangetoond worden in hoeverre SIO Noord-Holland voldoet aan de AVG.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekortschieten, dan kan SIO Noord-Holland de betrokken verantwoordelijke medewerkers een maatregel opleggen, binnen de kaders van de cao en de wettelijke mogelijkheden.

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten SIO Noord-Holland maken het noodzakelijk om periodiek te bezien of het beleid nog voldoet.

Bijlage 1: Taken van medewerkers

Onderstaand overzicht geeft de relaties tussen de three lines of defence aan bij een aantal AVG gerelateerde onderwerpen.

Onderwerp	Verantwoordelijk voor	Rol/functie
IBP-beleid	Vaststellen	Bestuurder en GMR
	Evalueren en bijstellen	Werkgroep Privacy
Handboek Privacy	Vaststellen	Bestuurder en GMR
	Evalueren en bijstellen	Werkgroep Privacy
	Bespreken en tips, aanvullingen doorgeven aan Privacy Officer	Directeur
	Toetsen naleving en werking handboek	FG
Toestemming	Toestemming vragen aan ouders en indien via de app Parro ouders hieraan jaarlijks herinneren	Directeur
Voorlichting en naleving	Voorlichting en bewustwording medewerkers	Directeur
	Communicatie handboek naar medewerkers	Directeur
	Toezien op naleving handboek	Directeur
Document- en datamanagement	Toepassen van technische beveiligingsmaatregelen (back-up, encryptie, etc.)	Bovenschoolse ICT er Cloudwise ICT-werkgroep
	Vaststellen bewaarplaatsen op school	Directie/IB
	Vernietiging persoonsgegevens conform bewaartermijnen	Directeur
Toegangsbeleid	Doorvoeren autorisaties (rollen en bevoegdheden) in systemen, bijv. ParnasSys	Directeur
	Toetst naleving en werking toegangsbeleid	FG
Verwerkersovereenkomsten	Doorgeven nieuwe verwerkers (leveranciers) aan bestuurssecretariaat	Directeur
	Afsluiten verwerkersovereenkomsten	Bestuurder
	Opvragen verwerkersovereenkomsten voor individuele scholen en doorgeven aan bestuurssecretariaat	Directeur
	Toetsen verwerkersovereenkomsten op rechtmatigheid en volledigheid	FG
Datalekken	Datalekken doorgeven aan Meldpunt (Privacy Officer)	Medewerkers (Ontdekkers)

	Verzamelen meldingen en benodigde informatie	Privacy Officer
	Melden bij FG en registreren	Privacy Officer
	Afweging maken tot melding Autoriteit Persoonsgegevens	FG i.o.m. Bestuurder
	Melding maken bij Autoriteit Persoonsgegevens	FG
Devices in bruikleen	Afsluiten gebruikersovereenkomst voor devices die in bruikleen worden gegeven bij leerlingen en medewerkers.	Directeur
DPIA	Uitvoeren wettelijk verplichte risicoanalyse (DPIA)	Directeur, Bovenschoolse ICT er, Privacy Officer
	Advisering bij uitvoering DPIA	FG
Rechten betrokkenen	Verzoek tot inzage, verwijdering of aanpassing persoonsgegevens afhandelen	Directeur
	Toetsen naleving procedure rechten betrokkenen	FG
Vastlegging verwerkingen (Dataregister)	Vastlegging verwerkingen persoonsgegevens conform artikel 30 AVG in een dataregister.	Privacy Officer
	Toetsen of vastlegging voldoet aan wet- en regelgeving	FG

9. Privacyreglement SIO Noord-Holland

Versie: 1

Vastgesteld op: september 2022

Privacy reglement

Stichting Islamitisch Onderwijs Noord-Holland

Inleiding

ICT is noodzakelijk in het verzorgen van het onderwijs. Wij werken met persoonsgegevens (van onszelf, leerlingen en anderen). Bovendien leggen wij systematisch veel persoonsgegevens vast. Daarmee hebben wij te maken met de privacywetgeving. Deze wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen genomen moeten worden om de persoonsgegevens te beschermen. Dit protocol beschrijft hoe binnen ons bestuur wordt omgegaan met de verwerking van persoonsgegevens en de beveiliging van de informatie. Dit protocol is onderdeel van het IPB Handboek voor medewerkers. Hierin staan naast dit protocol praktische afspraken over onder andere gegevensopslag, omgang met sociale media en internet alsmede toestemming voor beeldmateriaal van leerlingen. Met dit document wordt voldaan aan de wettelijke informatieplicht conform Algemene Verordening Gegevensbescherming (AVG) die in 2018 is ingegaan.

Dit document wordt jaarlijks herzien.

1. Privacy van leerlingen en hun ouders

Om onze onderwijsdoelstelling te realiseren is het van belang goed te weten wie de leerling is, wat zijn talenten en uitdagingen zijn en hoe het onderwijs voor deze leerling het beste kan worden verzorgd. Om hier een beeld van te krijgen worden persoonlijke gegevens van die leerling op school verzameld en bewaard. In dit hoofdstuk is te lezen om welke verzamelingen dit gaat, waarom die gegevens worden gebruikt, wie ze gebruikt en aan wie ze worden verstrekt.

1.1. Welke persoonsgegevens?

Voor een adequaat onderwijsproces voor de leerling tijdens zijn schoolcarrière worden gegevens verzameld om de leerling optimaal te laten functioneren, zowel wat betreft prestaties als welbevinden. Deze gegevens worden vastgelegd in een leerlingdossier. De gegevens die worden verzameld en opgeslagen zijn:

- Naam, voornamen, geboortedatum, geslacht, geboorteland, nationaliteit, adresgegevens en soortgelijke voor communicatie benodigde gegevens van de leerling
- Administratienummer (o.a. BSN)
- Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling
- Gegevens over de aard en het verloop van het onderwijs, alsmede de behaalde resultaten en gegevens over verlof en verzuim
- Gegevens over de organisatie van het onderwijs, zoals welke klas, vakken en dergelijke
- Zorggegevens die nodig zijn voor de organisatie van het onderwijs (recht op meer tijd, klasorganisatie, etc.)
- Gegevens van psychosociale aard, zoals testrapporten, persoonlijkheidsonderzoeken, intelligentieonderzoeken en orthopedagogische onderzoeken
- Ontwikkelingsperspectiefplannen van de leerling
- Gespreksverslagen
- Verslaglegging van het multidisciplinair overleg (MDO)
- Gegevens nodig voor het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten
- Logingegevens over gebruik van de systemen

Deze gegevens worden zowel digitaal als op papier opgeslagen.

1.2. Wat is het doel van de verzameling van deze gegevens?

Deze gegevens worden verzameld om:

- Overzicht te hebben van de leerlingen die onderwijs volgen
- Overzicht te hebben van de aard, organisatie en verloop van dat onderwijs per leerling en de behaalde studieresultaten
- Te communiceren met leerlingen en/of hun ouders/ verzorgers
- Persoonlijke (waaronder medische) omstandigheden van een leerling en de gevolgen daarvan voor het volgen van onderwijs bij te houden
- Financieel beheer uit te kunnen voeren
- Aan de wettelijke eisen rond monitoring en verantwoording naar toezichthoudende instanties en zorginstellingen te kunnen voldoen
- Toegang tot de systemen te krijgen
- De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het bewaken van de consistentie en betrouwbaarheid van de opgeslagen gegevens te verzorgen

- De continuïteit en goede werking van de systemen te waarborgen

1.3. Wie hebben toegang tot de leerlinggegevens en hoe worden deze beveiligd?

Binnen de school hebben de volgende type medewerkers toegang tot (een deel van) de gegevens:

- Leden van het CvB, de directie en het MT
- Onderwijzend personeel
- Onderwijsondersteunend personeel (OOP: administratief, zorgcoördinator, IB, ICT ondersteunend, SMW, logopedist, orthopedagoog en stafmedewerkers)

Niet alle medewerkers hebben toegang tot alle gegevens . Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren.

Gegevens die daarbij niet noodzakelijk zijn, zijn door die rol ook niet in te zien of te wijzigen. Gegevens met betrekking tot administratie, inschrijving, onderwijsbegeleiding en zorg worden in ParnasSys opgeslagen. Voor ParnasSys is een toegangsbeleid opgesteld waarin is vastgelegd welke functies tot welke gegevens toegang mogen hebben. Dit beleid wordt jaarlijks gecontroleerd. Gegevens worden indien nodig ingescand en in ieder geval digitaal opgeslagen. Hiertoe hebben alleen medewerkers toegang die deze gegevens nodig hebben bij het uitvoeren van hun werkzaamheden.

In het Handboek Privacy is een overzicht opgenomen van de verschillende functies en welke gegevens zij kunnen inzien en/of wijzigen. Inloggen in ParnasSys is alleen voorbehouden aan medewerkers die in dienst zijn van het bestuur en externe zorgbegeleiders. Met de leveranciers van ParnasSys zijn zogenaamde verwerkersovereenkomsten (conform het model van de PO-raad) afgesloten, waarin ook afspraken zijn gemaakt over beveiliging en back-up van de data die in ParnasSys wordt opgeslagen.

De uitwisseling met de overheid en andere scholen gebeurt ook middels ParnasSys. Deze systemen voldoen om deze reden ook aan de nationale standaarden op het gebied van beveiliging die de overheid heeft bepaald.

Voor digitale leermiddelen en toetsen worden systemen van diverse leveranciers of uitgeverijen gebruikt. Met deze partijen worden of zijn verwerkersovereenkomsten afgesloten. Onderdeel hiervan is dat zij ook voldoen aan de nationale standaarden en voorzieningen met betrekking tot de veilige uitwisseling van persoonsgegevens. In dit kader zal op termijn gebruik worden gemaakt van de nummervoorziening die het mogelijk maakt om alleen nog maar gepseudonimiseerde gegevens met deze partijen uit te wisselen. Meer informatie hierover is hier te vinden.

Een overzicht van leveranciers met wie een overeenkomst is afgesloten over de uitwisseling van persoonsgegevens is op te vragen bij de betreffende school.

1.4. Aan wie worden deze gegevens verstrekt?

De gegevens mogen in beginsel niet aan derden worden doorgegeven of door anderen worden ingezien zonder toestemming van de ouders, tenzij de school verplicht is om bepaalde persoonsgegevens te verstrekken, die noodzakelijk zijn voor de uitvoering van een wettelijke plicht. Toestemming van ouders vindt schriftelijk plaats en wordt opgeslagen in het leerlingdossier. Bij het uitwisselen van gegevens wordt altijd gecheckt of aan de vijf privacy-vuistregels wordt voldaan:

1. Doel en doelbinding

2. Grondslag
3. Dataminimalisatie
4. Transparantie
5. Data-integriteit

De gegevens worden verstrekt aan de volgende externe partijen:

- Externe partijen die in opdracht van de school en met toestemming van de ouders ondersteunen bij het bieden van aanvullende onderwijsbegeleiding voor de leerling.
- Een andere onderwijsinstelling bij verhuizing, overplaatsing of doorstroming naar het V(S)O. Ouders hoeven hiervoor geen toestemming te verlenen. Zij hebben wel recht op inzage. Eventuele opmerkingen van ouders kunnen toegevoegd worden aan het dossier, maar de school is niet verplicht tot wijziging van de gegevens.
- Het Regionaal Samenwerkingsverband. Ook hiervoor hoeven ouders geen toestemming te verlenen. Zij hebben wel recht op inzage. Eventuele opmerkingen van ouders kunnen toegevoegd worden aan het dossier, maar de school is niet verplicht tot wijziging van de gegevens.
- Externe deskundigen uit het MDO (schoolmaatschappelijk werk, schoolarts/ -verpleegkundige, ambulant begeleider, orthopedagoog) op grond van toestemming door de ouders/verzorgers.
- Externe partijen die in opdracht van de school en met toestemming van de ouders ondersteunen bij het bieden van aanvullende zorg voor de leerling.
- Bewerkers in de zin van leveranciers van onderwijsmiddelen die in opdracht van de school zorgen voor toegang en beheer van de digitale systemen die bij de begeleiding en zorg voor leerlingen worden gebruikt en waarmee een verwerkersovereenkomst is afgesloten.
- De Inspectie van het Onderwijs op grond van een wettelijke verplichting inzake onderwijskwaliteit.

1.5. Inzage en wijzigen

Wanneer men de persoonsgegevens wil inzien of wijzigen, dan kan men hiervoor een afspraak maken met de directeur van de betreffende school. Afhankelijk van de werkzaamheden die nodig zijn voor het beschikbaar stellen van gegevens, kan er een vergoeding gevraagd worden van max. €5,00. Dit geldt uiteraard niet voor het doorgeven van wijzigingen. Ouders krijgen het dossier niet mee, maar hebben wel recht op een kopie.

1.6. Bewaartermijnen

De persoonsgegevens van leerlingen worden uiterlijk 2 jaren na de uitschrijving van een leerling verwijderd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan de wettelijke bewaarplicht.

2. Privacy van medewerkers

Wij verwerken ook de persoonsgegevens van onze medewerkers binnen het bestuur. Soms zijn dat gegevens die direct samenhangen met de arbeidsverhouding tussen het bestuur en medewerkers, maar ook worden persoonsgegevens van onze medewerkers verwerkt in systemen die gebruikt worden bij het geven en begeleiden van onderwijs. De informatie over persoonsgegevens van medewerkers is ook van toepassing op stagiaires.

In dit hoofdstuk is te lezen om welke verzamelingen het gaat, waarom die gegevens worden gebruikt, wie ze gebruikt en aan wie ze worden verstrekt.

2.1. Welke gegevens?

- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie benodigde gegevens, bankrekeningnummer van de medewerker
- Een administratienummer (o.a. BSN)
- Nationaliteit en geboorteplaats
- Gegevens voor digitale communicatie
- Gegevens over de groep waar een medewerker aan gekoppeld is
- Gegevens over het gebruik van de systemen
- Gegevens over salaris, belasting, premies en andere vergoedingen
- Gegevens over gevolgde en te volgen opleidingen, cursussen en stages
- Gegevens voor personeelsbeoordeling en loopbaanbegeleiding, voor zover die gegevens bij de medewerker bekend zijn
- Gegevens over de (voormalige) functie, alsmede over de aard, inhoud en beëindiging van het dienstverband
- Gegevens voor de administratie van aan- en afwezigheid, in verband met verlof, arbeidsduurverkorting, bevalling of ziekte, met uitzondering van gegevens over de aard van de ziekte
- Gegevens die in het belang van de medewerker worden opgenomen met het oog op zijn/haar arbeidsomstandigheden
- Gegevens, waaronder begrepen gegevens over (voormalige) gezinsleden van de medewerker, die noodzakelijk zijn voor een overeengekomen arbeidsvoorwaarde
- Andere dan de hierboven genoemde gegevens waarvan de verwerking wordt vereist vanwege de toepassing van een andere wet

2.2. Wat is het doel van de verzameling van deze gegevens?

Deze gegevens worden verzameld om:

- Onderwijs te geven en leerlingen te begeleiden en volgen, waaronder:
  - Opslag van leer- en toetsresultaten
  - Het terugontvangen van leer- en toetsresultaten om te verwerken in het leerlingvolgsysteem
  - De beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen aanbieden dat is afgestemd op de specifieke leerbehoefte van een leerling
  - Analyse en interpretatie van leerresultaten
  - Het kunnen uitwisselen van leer- en toetsresultaten tussen digitale onderwijsmiddelen

    - Gebruik te maken van specifiek leerkrachten-informatie in de digitale onderwijsmiddelen
- (Digitale) onderwijsmiddelen door leveranciers geleverd te krijgen en in gebruik te kunnen nemen
- Het geven van leiding aan de werkzaamheden van de medewerker
- De behandeling van personeelszaken
- Het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura
- Het berekenen, vastleggen en betalen van belasting en premies
- De uitvoering van een voor de medewerker geldende arbeidsvoorwaarde
- Opleidingen en scholing van de medewerker
- Bedrijfsmedische zorg en bedrijfsmaatschappelijk werk voor de medewerker
- Het opstellen van een lijst van data van verjaardagen en andere feestelijkheden en gebeurtenissen
- De interne controle en de bedrijfsvoering
- Het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen
- Het behandelen van geschillen
- Het doen uitoefenen van accountantscontrole
- Het verlenen van ontslag
- Het regelen van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband
- De uitvoering of toepassing van een andere wet
- Toegang tot de systemen te krijgen
- De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het bewaken van de consistentie en betrouwbaarheid van de opgeslagen gegevens te verzorgen
- De continuïteit en goede werking van de systemen te waarborgen

Voor de organisatie van het onderwijs en begeleiding van leerlingen wordt gebruikgemaakt van digitale systemen, waarin gegevens over hun prestaties en welbevinden worden vastgelegd. In deze systemen worden ook gegevens van onderwijzend personeel vastgelegd, gericht op het kunnen maken van een koppeling tussen leerling en leerkracht en om de opgeslagen gegevens van de leerlingen in te kunnen zien, aan te vullen en te wijzigen.

Voor het verzorgen van het onderwijs wordt, naast boeken, ook gebruikgemaakt van digitale onderwijsmiddelen. In deze onderwijsmiddelen, die worden afgenomen van externe leveranciers, worden persoonsgegevens verwerkt die nodig zijn voor de toegang tot en het gebruik van deze digitale producten en diensten. Voorbeelden van deze digitale onderwijsmiddelen zijn: digitale (aanvullingen op) lesmethodes, toetssystemen en apps. Ook in deze systemen worden persoonsgegevens van onderwijzend personeel opgeslagen.

Tevens worden onderwijsondersteunende ICT-middelen, zoals Chromebooks of andere (draagbare) computersystemen ingezet. Voor systeembeheer, beveiliging, logging en monitoring wordt software op deze middelen geïnstalleerd die persoonsgegevens verzamelen.

2.3. Wie hebben toegang tot de personeelsgegevens en hoe worden deze beveiligd?

Binnen de school hebben de volgende type medewerkers toegang tot (een deel van) de gegevens:

- Leden van het CvB, de directie en het MT (systemen voor organisatie en begeleiding onderwijs en formatieplanning)

- Administratief personeel (systemen voor organisatie en begeleiding onderwijs en formatieplanning)
- Stafmedewerker bestuursbureau, directiesecretaresses (alleen het systeem voor formatieplanning) en hoofd bedrijfsvoering
- Medewerkers salarisadministratie en financiën
- Personeelsadviseurs
- Leidinggevende van de betreffende medewerker
- Hoofd P&O, bedrijfsvoering en financiën
- ICT-ondersteunend personeel

Niet alle rollen hebben toegang tot alle gegevens. Per rol is vastgesteld welke gegevens ingezien en gewijzigd kunnen worden, waarbij is gekeken wat die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, zijn door die rol ook niet in te zien of te wijzigen. Voor personeelsgegevens die in dezelfde systemen worden verwerkt als die van leerlingen, gelden dezelfde maatregelen als in hoofdstuk 1.3. Via SIO Noord-Holland worden verzuimgegevens geregistreerd. Ook hiervoor geldt dat er binnen het bestuur een toegangsbeleid is opgesteld dat jaarlijks wordt gecontroleerd voor het digitaal administratiesysteem. Met de leverancier hiervan is een verwerkersovereenkomst afgesloten.

2.4. Aan wie worden deze gegevens verstrekt?

De gegevens worden verstrekt aan de volgende externe partijen:

- Bewerkers in de zin van leveranciers van onderwijsmiddelen en of die in opdracht van de school deze middelen ter beschikking stellen
- Bewerkers die zorgen voor toegang tot de onderwijsmiddelen in opdracht van de school
- Bewerkers in de zin van leveranciers van onderwijsmiddelen die in opdracht van de school zorgen voor toegang en beheer van de digitale systemen die worden gebruikt bij de begeleiding en zorg voor leerlingen

2.5 Inzage en wijziging

Alle medewerkers binnen het bestuur hebben een eigen inlog voor het digitale personeelsdossier. Wanneer men vragen heeft over de persoonsgegevens of deze wil wijzigen dan kan men terecht bij de administratie van het bestuur, te bereiken via telefoonnummer: 020-362 0889. Wanneer men de persoonsgegevens wil inzien of wijzigen in de onderwijssystemen van de school, dan kan men hiervoor terecht bij de afdeling administratie van de betreffende school.

2.6 Bewaartermijnen

De persoonsgegevens van medewerkers worden uiterlijk 2 jaar na de beëindiging van het dienstverband van de medewerker verwijderd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan de wettelijke bewaarplicht.

3. Privacy van derden

In sommige gevallen worden gegevens van derden opgeslagen, die geen leerling, ouder of medewerker zijn. Denk bijvoorbeeld aan sollicitanten en extern ingehuurd personeel. In dit hoofdstuk is te lezen om welke verzamelingen dit gaat, waarom die gegevens worden gebruikt, wie ze gebruikt en aan wie ze worden verstrekt.

3.1. Sollicitanten

In een sollicitatieproces worden persoonsgegevens verwerkt van sollicitanten. Deze paragraaf beschrijft hoe binnen ons bestuur met deze gegevens wordt omgegaan. De gegevens die worden verzameld en opgeslagen zijn:

- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie benodigde gegevens, bankrekeningnummer van de medewerker
- Een administratienummer (o.a. BSN)
- Nationaliteit en geboorteplaats
- Gegevens over gevolgde en te volgen opleidingen, cursussen en stages
- Gegevens over de functie waarnaar gesolliciteerd is
- Gegevens over de aard, inhoud van huidige en vorige dienstverbanden en beëindiging van vorige dienstverbanden
- Andere gegevens met het oog op het vervullen van de functie, die door de sollicitant zijn verstrekt of die hem of haar bekend zijn (testen, assessments, etc.)
- Andere dan de hierboven genoemde gegevens waarvan de verwerking wordt vereist vanwege de toepassing van een andere wet

Deze gegevens worden verzameld om:

- De geschiktheid van een sollicitant te beoordelen voor een functie die vacant is of kan komen
- De veiligheid binnen de organisatie te borgen
- De door de sollicitant gemaakt onkosten af te handelen
- De uitvoering of toepassing van een andere wet te borgen

Binnen het bestuur hebben alleen medewerkers die betrokken zijn bij de sollicitatieprocedure toegang tot de persoonsgegevens van de sollicitanten. De gegevens worden alleen verstrekt aan externe partijen die namens het bestuur een test of assessment verzorgen. In dat geval worden aan de direct bij de activiteiten betrokken personen slechts de persoonsgegevens verstrekt die noodzakelijk zijn voor de test of assessment.

3.2. Bijzonderheden

De persoonsgegevens worden verwijderd op een daartoe strekkend verzoek van de sollicitant en in ieder geval uiterlijk vier weken nadat de sollicitatieprocedure is beëindigd, tenzij de persoonsgegevens met toestemming van de sollicitant langer worden bewaard.

3.3. Inzage en wijziging

Alle medewerkers binnen het bestuur hebben een eigen inlog voor het digitale personeelsdossier. Wanneer men vragen heeft over de persoonsgegevens of deze wil wijzigen, dan kan men hiervoor terecht bij de afdeling personeelszaken.

3.4 Extern ingehuurd personeel

Soms wordt gebruikgemaakt van extern personeel, om kennis aan te vullen of om opengevallen plekken tijdelijk op te vullen. Om de contracten en inzet af te handelen, worden gegevens in diverse systemen opgeslagen. Persoonsgegevens De gegevens die worden verzameld en opgeslagen zijn:

- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie bedoelde gegevens
- Bedrijfsgegevens en bankrekeningnummer van de extern ingehuurde medewerker
- Kopie verstrekte VOG
- De gegevens voor de organisatie en begeleiding van onderwijs zoals vermeld in paragraaf 2.1.

Deze gegevens worden verzameld om:

- De contractuele en financiële verplichtingen af te handelen die samenhangen met de inhuur
- De ingehuurde in staat te stellen de ICT-middelen en software in te zetten die nodig zijn bij de uitvoer van de werkzaamheden
- De correcte uitvoering van een wettelijke verplichting die samenhangt met de inhuur.

Binnen de school hebben de volgende type medewerkers toegang tot de gegevens:

- Medewerkers salarisadministratie en financiën
- Personeelsadviseurs
- Opdrachtgever van de betreffende externe medewerker
- Hoofd P&O, bedrijfsvoering en financiën
- ICT-ondersteunend personeel

Deze gegevens worden verstrekt aan uitzendbureaus en detacheringsbureaus waarmee door het bestuur wordt samengewerkt.

3.5 Bijzonderheden

De persoonsgegevens worden verwijderd zo snel mogelijk na beëindiging van de contractperiode, maar maximaal na 2 jaar, tenzij een wettelijke bepaling anders voorschrijft.

3.6 Inzage en wijziging

Wanneer men de persoonsgegevens wil inzien of wijzigen, dan kan men hiervoor terecht bij de afdeling personeelszaken.

3.7 Vrijwilligers

Vrijwilligers, met name ouders van (oud)leerlingen, worden op de verschillende scholen ingezet om te helpen bij schoolactiviteiten zoals sportdagen en excursies. Van de vrijwilligers worden alleen gegevens verzameld en opgeslagen die nodig zijn om contact met hen te onderhouden. Het betreft

naam, adres, telefoonnummer en/of e-mailadres. Voor inzage en wijziging kan de betreffende vrijwilliger terecht bij de administratie van de school waar hij of zij vrijwilligerswerk verricht.

3.8. Oud-leerlingen

Voor het onderhouden van contacten met en het verzenden van informatie aan oud-leerlingen worden de volgende gegevens opgeslagen:

- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie bedoelde gegevens
- Gegevens betreffende de schoolloopbaan van de oud-leerling.

4. Datalekken

Wanneer de kans bestaat dat er persoonsgegevens in handen zijn gekomen van derden die geen toegang zouden moeten hebben tot die gegevens of wanneer de mogelijkheid bestaat dat er persoonsgegevens verloren zijn gegaan dient dit direct gemeld te worden bij het bevoegd gezag. Het bevoegd gezag is verantwoordelijk voor eventuele melding van een datalek bij de Autoriteit Persoonsgegevens, indien er onterecht geen melding gedaan wordt kan dit leiden tot fikse boetes.

De volledige Procedure Melden Datalekken is opgenomen in de Procedure Melden Beveiligingsincidenten en Datalekken.

5. Klachten

Indien men van mening is dat het privacy protocol niet op de juiste wijze wordt nageleefd binnen het bestuur kan er een klacht worden ingediend bij privacy@sionoord-holland.nl. Wanneer deze klacht voor de betrokkene niet leidt tot een acceptabele oplossing kan men zich wenden tot het bestuur of de Functionaris Gegevensbescherming via fg@sionoord-holland.nl.

10. Procedure melden beveiligingsincidenten en datalekken SIO Noord-Holland

Bron:
Kennisnet

Bewerkt door:
SIO Noord-Holland

Versiebeheer:

Versie	Status	Datum	Naam	Omschrijving
1	concept	november 2022	Haci Karacaer	

1. Vooraf

Dit protocol wordt gehanteerd bij het melden en afhandelen van (mogelijke) beveiligingsincidenten binnen SIO Noord-Holland of (mogelijke) beveiligingsincidenten die buiten onze organisatie hebben plaatsgevonden, maar waarvoor SIO Noord-Holland als verwerkingsverantwoordelijke verantwoordelijkheid draagt (bijvoorbeeld als een beveiligingsincident zich bij een verwerker van SIO Noord-Holland voordoet). In het protocol is vastgelegd hoe en naar wie de meldingen intern doorgezet dienen te worden, wie verantwoordelijk is voor welke melding en hoe de melding aan de Autoriteit Persoonsgegevens (AP) en eventueel ook aan de betrokkenen wordt gedaan.

2. Inleiding

Regelmatig lezen we in de media dat gegevens van werknemers, studenten of patiënten letterlijk op straat liggen; dossiers die worden aangeboden als oud papier, een gestolen smartphone of een verloren USB-stick. Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, spreken we van een datalek. Het risico op datalekken wordt steeds groter omdat onze persoonsgegevens in steeds meer databanken en/of op informatiedragers zijn opgeslagen. Een datalek kan nadelige gevolgen hebben voor de privacy van degene van wie de persoonsgegevens zijn gelekt. Weggelekte persoonsgegevens kunnen oneigenlijk gebruikt worden. Identiteitsfraude is hier een voorbeeld van.

We kunnen drie categorieën datalekken onderscheiden:

- Inbreuk op de vertrouwelijkheid; Als er sprake is van een onbevoegde of onopzettelijke toegang tot of openbaring van persoonsgegevens
- Inbreuk op de integriteit; Als er sprake is van onbevoegd of onopzettelijk wijzigen van persoonsgegevens.
- Inbreuk op de beschikbaarheid; Wanneer de toegang tot persoonsgegevens niet meer mogelijk is of persoonsgegevens vernietigd zijn.

In de AVG is de meldplicht voor datalekken opgenomen in artikel 33 en 34. Deze meldplicht verplicht organisaties, dus ook scholen, om datalekken te melden bij de toezichthouder, de Autoriteit Persoonsgegevens (AP) en, in sommige gevallen, ook bij de betrokkenen (de personen op wie de gegevens die zijn gelekt betrekking hebben).

Indien de meldplicht aan betrokkene en/of de Autoriteit Persoonsgegevens niet wordt nagekomen riskeert SIO Noord-Holland een hoge boete die kan oplopen tot maximaal 10 miljoen euro of 2% van de totale omzet (artikel 83, lid 4 AVG). Alleen die inbreuken die waarschijnlijk leiden tot een risico voor de rechten en vrijheden van de betrokkenen, moeten bij de AP worden gemeld. Door deze clausulering worden inbreuken met geringe nadelige gevolgen voor de bescherming van persoonsgegevens uitgezonderd van de meldplicht, maar moeten wel door SIO Noord-Holland geregistreerd worden in een register voor beveiligingsincidenten.

3. Begripsbepalingen

In dit protocol worden onder meer de volgende termen gebruikt:

- Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. In ons geval gaat het dan om leerlinggegevens, gegevens van ouders, leerkrachten en van de personen die voor ons werkzaam zijn;
- Betrokkene: de persoon op wie de persoonsgegevens betrekking hebben;

- Beveiligingsincident: een gebeurtenis (niet uitsluitend digitaal!) die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de Informatievoorziening wordt aangetast;
- Informatievoorziening: het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie;
- Datalek: een beveiligingsincident (niet uitsluitend digitaal!) waarbij persoonsgegevens verloren raken of onrechtmatig worden verwerkt (denk aan: opgeslagen, aangepast, verzonden, et cetera) of als dit niet uit te sluiten is. Of anders gezegd: een inbreuk op de informatiebeveiliging waarbij persoonsgegevens verloren gaan of in handen komen van derden die geen toegang tot die gegevens mogen hebben, of dat toegang door onbevoegden niet uitgesloten kan worden.

Alle datalekken zijn dus beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken. Bij ieder beveiligingsincident zal moeten worden vastgesteld of er sprake is van een datalek.

4. Rollen bij een (mogelijk) beveiligingsincident

SIO Noord-Holland onderscheidt vier rollen om een (mogelijk) beveiligingsincident succesvol af te handelen:

- De Ontdekker: degene die een (mogelijk) beveiligingsincident op het spoor komt en het proces in werking stelt. Dat kan dus iedere medewerker zijn, maar ook ouders of relaties (verwerkers). Indien een ouder, leerling, relatie of andere derde een (mogelijk) beveiligingsincident opmerkt, is het van belang dat hij/zij dit onmiddellijk meldt bij de directeur van de school.
- Het Meldpunt: de centrale locatie binnen SIO Noord-Holland waar alle (mogelijke) beveiligingsincidenten door de ontdekker moeten worden gemeld. De gegevens over het (mogelijk) beveiligingsincident worden geregistreerd en verder verwerkt in een register voor beveiligingsincidenten. Het meldpunt is bereikbaar via het e-mailadres privacy@sionoord-holland.nl of direct via de directeur van de school.
- De Melder (FG): degene die namens de verwerkingsverantwoordelijke (bestuur van SIO Noord-Holland) verantwoordelijk is voor het beoordelen van het beveiligingsincident en het – op het besluit van het bestuur - eventueel melden van een datalek bij de Autoriteit Persoonsgegevens en (indien van toepassing) aan de Betrokkene(n). De melder is bij SIO Noord-Holland de Functionaris voor Gegevensbescherming (FG).
- De (bovenschoolse) ICT-coördinator: degene die in het geval van digitale (mogelijke) beveiligingsincidenten de melder ondersteunt bij het onderzoek naar de oorzaak van het beveiligingsincident en het (laten) repareren van het beveiligingsincident en/of het beperken van de gevolgen daarvan. Hierbij zal ook de ICT/netwerkleverancier betrokken worden.

5. Stappenplan bij een (mogelijk) beveiligingsincident

1. Ontdekken: door alle medewerkers en externen

De ontdekker merkt een (mogelijk) beveiligingsincident op. Dit kan via eigen waarneming of via waarneming van een derde. De ontdekker kan een medewerker, maar ook een ouder, leerling of relatie (verwerker) zijn.

De ontdekker meldt het door hem of haar opgemerkte (mogelijke) beveiligingsincident direct bij het meldpunt via privacy@sionoord-holland.nl of bij de directeur van de school. In het geval van e-mailen wordt in het onderwerp van de e-mail "(mogelijk) Beveiligingsincident" en de naam van de school vermeld, zodat voor het meldpunt direct duidelijk is waar het om gaat. Bovendien moet de e-mail als "urgent" worden verzonden.

2. Inventariseren en vastleggen: door het meldpunt

Het meldpunt (Privacy Officer) verzamelt zo spoedig mogelijk alle relevante informatie met betrekking tot het (mogelijke) beveiligingsincident en legt e.e.a. vast. Het meldpunt kan daarvoor aanvullende vragen uitzetten bij de ontdekker of de ICT/netwerkleverancier.

De volgende informatie wordt door het meldpunt verzameld en vastgelegd:

- Een samenvatting van het beveiligingsincident; waar heeft het incident plaatsgevonden en wat is er met de gegevens gebeurd;
- Aard van de inbreuk;
- Datum/periode van het beveiligingsincident;
- Vond het beveiligingsincident plaats in een verwerking die is uitbesteed aan een andere organisatie (een verwerker), zo ja, wat is de naam van de verwerker;
- Een nadere omschrijving van:
  - De categorieën van betrokkenen (leerlingen, ouders, leerkrachten etc.);
  - (Bij benadering) het aantal betrokkenen;
  - Type persoonsgegevens (bijzondere gegevens of van gevoelige aard?);
  - Worden de gegevens binnen een keten gedeeld;
  - Indien van toepassing, binnen welke keten de persoonsgegevens in kwestie worden gedeeld;
  - De vooralsnog bekende en/of te verwachten gevolgen die het beveiligingsincident voor de persoonlijke levenssfeer van de betrokkenen kan hebben;
  - De mogelijke technische beschermingsmaatregelen die zijn genomen (denk aan versleuteling, encryptie, hashing etc.);
  - De technische en organisatorische maatregelen die zijn getroffen om het beveiligingsincident aan te pakken.

Alle informatie die wordt verzameld dient schriftelijk te worden vastgelegd. Hiervoor wordt het register voor beveiligingsincidenten.

Wanneer het meldpunt voldoende informatie heeft verzameld, stuurt het meldpunt de melder (FG) een verzoek om de verzamelde informatie te bekijken.

3. Beoordelen: door de melder (FG)

De melder (FG) beoordeelt de feiten om te bepalen of er sprake is van een beveiligingsincident en zo ja, of dit beveiligingsincident is aan te merken als een datalek. Door de melder moeten de volgende vragen worden beantwoord:

- Is er sprake van een datalek?
- Wordt het datalek gemeld aan de AP? Waarom wel/niet?
- Wordt het datalek aan betrokkene(n) gemeld? Waarom wel/niet?

De FG deelt de bevindingen met de bestuurder.

Eerst wordt beoordeeld of er sprake is van een datalek. Indien er sprake is van een datalek, beoordeelt de melder vervolgens of het datalek moet worden gemeld aan de Autoriteit Persoonsgegevens. Immers, niet alle datalekken hoeven te worden gemeld aan de AP. Volgens de wet moet een "ernstig" datalek worden gemeld aan de AP. Een datalek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig). Daarnaast kan een datalek ook ernstig zijn indien er geen grote hoeveelheden persoonsgegevens gelekt zijn, maar het wel om gevoelige persoonsgegevens gaat (kwalitatief ernstig). Dit laatste is bijvoorbeeld het geval als het gaat om bijzondere persoonsgegevens, persoonsgegevens over de financiële of economische situatie van de betrokkene(n), of als de gegevens kunnen leiden tot stigmatisering van de betrokkene(n).

De aard (het type) en de omvang (de hoeveelheid) van het datalek spelen dus beide een belangrijke rol bij de beoordeling of melding aan de AP noodzakelijk is. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er gemeld worden. De onderstaande beslisboom kan hierbij gebruikt worden.

Indien er sprake is van een datalek dat gemeld moet worden aan de AP, beoordeelt de melder vervolgens of het datalek ook moet worden gemeld aan de betrokkene(n). Dit is namelijk niet automatisch het geval. Hiervoor moet onder andere worden gekeken of het datalek kan leiden tot fysieke, materiële of immateriële schade voor de betrokkene(n), zoals discriminatie, (identiteits-) fraude, financiële schade en reputatieschade. Als de betrokkene jonger is dan 16 jaar worden de ouders ingelicht.

De melding aan betrokkene(n) mag achterwege worden gelaten als:

- Er voordat het datalek plaatsvond passende maatregelen zijn getroffen waardoor de gelekte persoonsgegevens onbegrijpelijk zijn voor onbevoegden. Let op: deze uitzondering geldt alleen als de gegevens nog volledig intact zijn;
- Er nog steeds volledige controle is over de gegevens;
  - De sleutel die voor de encryptie of voor de hashing is gebruikt bij de inbreuk geen gevaar heeft gelopen en voor onbevoegden met de beschikbare technologische middelen niet te vinden is;
  - Er onmiddellijk nadat het datalek heeft plaatsgevonden, maatregelen zijn getroffen waardoor het hoge risico voor de rechten en vrijheden van betrokkene(n) zich waarschijnlijk niet meer zal voordoen (bijvoorbeeld doordat de gelekte persoonsgegevens onmiddellijk na het datalek zijn gewist, nog voordat de onbevoegde ontvanger iets met de gegevens kon doen);
- Wanneer het niet melden noodzakelijk en evenredig is ter waarborging van: a. de nationale veiligheid; b. landsverdediging; c. de openbare veiligheid; d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Bij ieder beveiligingsincident wordt beoordeeld of er aanwijzingen zijn voor of vermoedens van strafbaar handelen (zoals bijvoorbeeld hacken). Indien dit het geval is, kan aangifte worden gedaan bij de politie.

Als een ontdekker het niet eens is met de beslissing van de melder om een (vermoedelijk) datalek wel of niet te melden aan de Autoriteit Persoonsgegevens en/of de betrokkene(n), dan richt hij of zij zich tot het college van bestuur teneinde zijn of haar bedenkingen aldaar te bespreken. Het is de ontdekker (meestal medewerker) niet toegestaan om een (vermoedelijk) datalek zelf aan de Autoriteit Persoonsgegevens/of de betrokkene(n) te melden. Zie ook onder punt 5 bij “Communicatie”.

4. Maatregelen treffen: door de (bovenschoolse) ICT-coördinator in samenwerking met de ICT leverancier

De bovenschoolse ICT-coördinator wordt door het meldpunt en/of de melder gevraagd (voor zover dat nog niet is gebeurd en voor zover mogelijk) de oorzaak van het beveiligingsincident vast te stellen en (technische) maatregelen te treffen om het beveiligingsincident te (laten) verhelpen en de gevolgen van het beveiligingsincident te beperken. Ook wordt gevraagd om (technische) maatregelen te treffen om herhaling van het beveiligingsincident te voorkomen. Deze maatregelen worden zo spoedig mogelijk in gang gezet in samenwerking met de ICT/netwerk-leverancier.

5. Melden en communicatie: door de FG (melder)

Bij de Autoriteit Persoonsgegevens

Indien de conclusie bij stap 3 is dat er sprake is van een datalek dat bij de AP gemeld dient te worden, dan zal de FG dit in overleg met de bestuurder zo snel mogelijk doch liefst binnen 72 uur na het ontdekken van het datalek melden. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Als nog niet alle informatie over het datalek bekend is, zal alvast een incomplete melding worden gedaan, zodat de Autoriteit Persoonsgegevens tijdig is geïnformeerd. Ontbrekende informatie kan later worden toegevoegd. Het

datalek wordt gemeld bij het Meldloket datalekken Autoriteit Persoonsgegevens: https://datalekken.autoriteitpersoonsgegevens.nl

Communicatie naar betrokkenen

Indien de conclusie bij stap 3 is dat een datalek ook moet worden gemeld aan de betrokkene(n), dan moet dit zo snel mogelijk, liefst binnen een week, plaatsvinden. De melding aan betrokkene(n), dient in ieder geval behoorlijk en zorgvuldig uitgevoerd te worden, en de volgende informatie te bevatten:

- Aard van de inbreuk, waarbij volstaan kan worden met een algemene omschrijving van wat er is gebeurd;
- Waar men terecht kan met vragen, denk hierbij aan het telefoonnummer/e-mailadres van de FG of een speciaal telefoonnummer/e-mailadres voor vragen;
- Aanbevolen maatregelen om negatieve gevolgen te beperken, zoals het veranderen van wachtwoorden.

De betrokkene(n) dienen in beginsel individueel te worden geïnformeerd, maar als het individueel informeren van de betrokkene(n) een onevenredige inspanning vergt, bijvoorbeeld omdat de contactgegevens van de betrokkene(n) door het datalek verloren zijn gegaan, dan mogen de betrokkene(n) ook worden geïnformeerd met een openbare mededeling of een soortgelijke maatregel, waarbij de betrokkene(n) even doeltreffend worden geïnformeerd.

Overige Communicatie

Bij het melden aan de AP en eventueel de betrokkene(n) en/of de politie is de communicatie een belangrijk punt van aandacht. Het is van groot belang dat alle communicatie (zowel geschreven pers, sociale media platforms alsmede alle overige communicatieplatforms) uitsluitend via de melder en/of de bestuurder in onderling overleg plaatsvindt. Ieder ander dient zich te allen tijde te onthouden van enig commentaar en hiervoor te verwijzen naar de melder en/of de bestuurder van SIO Noord-Holland.

6. Vastleggen: door het Meldpunt

Alle informatie die in de voorafgaande stappen met betrekking tot een beveiligingsincident is ingewonnen of ontstaan, wordt door het meldpunt (in samenspraak met de melder) geregistreerd in het “register voor beveiligingsincidenten". Met deze registratie wordt het afhandelen van het beveiligingsincident afgesloten. Het meldpunt stuurt in overleg met de bestuurder een samenvatting van de genomen maatregelen aan de ontdekker.

6. Beheer beveiligingsincidenten

Het meldpunt maakt in samenwerking met de FG twee keer per jaar een analyse van alle meldingen van de beveiligingsincidenten die zij heeft ontvangen. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om extra maatregelen te nemen om herhaling te voorkomen. De GMR wordt geïnformeerd over de uitkomsten van de analyse.

7. Afspraken met leveranciers

Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Spreek af:

- Hoe informeer je elkaar over datalekken, en zorg ook voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatiegegevens de bewerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding (maak afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de bewerkers de gegevens moeten aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

Maak schriftelijke afspraken met uw bewerker(s) over datalekken. Hiervoor kan gebruik worden gemaakt van de model verwerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).