

IBP BELEID



Stroomm

INHOUDSOPGAVE

Hoofdstuk 1	Inleiding	3
Hoofdstuk 2	De basis van de privacywetgeving	4
Hoofdstuk 3	Privacyreglement en verklaring	7
Hoofdstuk 4	Toestemming foto's / video's en online diensten	7
Hoofdstuk 5	Rechten van betrokkenen en klachten over privacy	9
Hoofdstuk 6	Functionaris voor Gegevensbescherming	9
Hoofdstuk 7	Verwerkersovereenkomsten en verwerkersregister	10
Hoofdstuk 8	Procedure datalekken	11
Hoofdstuk 9	Toegangsbeleid	12
Hoofdstuk 10	Gedragscode	12
Hoofdstuk 11	Uitwisselen van gegevens	13
Hoofdstuk 12	Richtlijnen veilig mailen	14
Hoofdstuk 13	Bewaartermijnen	15
Hoofdstuk 14	Jaarplan privacy	16
Hoofdstuk 15	Geheimhouding	17
Hoofdstuk 16	DPIA	17
Hoofdstuk 17	Cameratoezicht	17
Bijlage 1	Persoonsgegevens	19
Bijlage 2	Procedure rechten van betrokkenen	20
Bijlage 2a	Inzage tabel	22
Bijlage 2b	Genomen stappen rechten van betrokkenen	23
Bijlage 3	Protocol datalekken	24
Bijlage 4	Toegangsmatrix	25

Hoofdstuk 1 Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. 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 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. Hiervoor is er binnen Stroomm een IBP-handboek opgesteld. Het IBP-handboek is op 10 juni 2025 vastgesteld door de GMR en op te vragen via privacy@stroomm.nl.

Dit handboek is bedoeld als informatiebron voor alle medewerkers van Stroomm. Hierin staan de afspraken die we met elkaar gemaakt hebben over informatiebeveiliging en privacy. Hierbij hebben wij naast de wettelijke basis, ook onze visie op onderwijs en onze normen en waarden als uitgangspunt genomen.



Hoofdstuk 2 De basis van de privacywetgeving

Privacy is een lastig en vaag begrip. Privacy op school gaat over de bescherming van gegevens over leerlingen, hun ouders en medewerkers. Dit wordt geregeld in de Algemene Verordening Gegevensbescherming (AVG). Als we praten over de AVG dan praten we over persoonsgegevens.

Wat zijn persoonsgegevens?

Een persoonsgegeven is informatie die direct iets over een persoon zegt of op een bepaalde manier herleidbaar is naar die persoon. Een andere manier om de term persoonsgegevens te omschrijven is: de gegevens waarmee je een specifiek persoon binnen een bepaalde groep kunt aanwijzen. Dat zijn bijvoorbeeld je naam, je adres en je geboortedatum. Bij een veel voorkomende naam, zullen er meestal wat gegevens moeten worden gecombineerd om een specifieke persoon aan te wijzen. Dat verandert niets aan het feit dat een naam altijd een persoonsgegeven is. In **Bijlage 1** Persoonsgegevens is te zien met welke type persoonsgegevens je te maken kunt hebben.

Grondslagen voor verwerking van persoonsgegevens

Je mag niet zomaar persoonsgegevens bewaren, verspreiden, bewerken etc. Dat mag alleen als er een grondslag op van toepassing is. Een grondslag is simpel gezegd een gegronde reden op basis waarvan je bevoegd bent om met de persoonsgegevens aan de slag te gaan. De AVG-wet noemt 6 grondslagen. Er moet altijd minimaal 1 grondslag van toepassing zijn voor je überhaupt iets mag doen met persoonsgegevens!

Om persoonsgegevens te mogen verzamelen hebben we dus een grondslag nodig. Deze zijn:

1. **Toestemming** van de betrokkene
Foto's, gebruik digitale middelen (sociale media), begeleiding leerling door externe onderwijsspecialist;
2. Noodzakelijk voor de **uitvoering van de overeenkomst**
Met de ouders/verzorgers. Bijvoorbeeld voor de TSO (tussenschoolse opvang) van kinderen, personeel de arbeidsovereenkomst;
3. Noodzakelijk voor voldoen aan een **wettelijke verplichting**
Bijvoorbeeld voor bekostiging, inspectie, overdrachtdossier;
4. Een **vitaal belang** te beschermen
De gegevensverwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen, bijvoorbeeld allergie;
5. Vervulling taak van **algemeen belang** of openbaar gezag
Bijvoorbeeld de uitwisseling van informatie met samenwerkingsverbanden (let op: geen BSN);
6. **Gerechtvaardigd belang**
Zoals het goed laten werken van digitale leermiddelen. Bijvoorbeeld voor Basispoort en educatieve uitgeverijen.

Vuistregels bij verzamelen en verstrekken van persoonsgegevens

Als er een grondslag is en je dus persoonsgegevens mag verwerken dan zijn de volgende vuistregels van belang:



1. Doelbepaling doelbinding

Worden de persoonsgegevens alleen gebruikt voor dat doel dat wij vooraf hebben vastgelegd?

Persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld.

De belangrijkste doelen zijn voor het onderwijs:

- de organisatie of geven van onderwijs;
- het leren en begeleiden van leerlingen/studenten;
- het verstrekken of ter beschikking stellen van leermiddelen;
- het bekend maken van informatie over de hierboven genoemde organisatie en leermiddelen; het bekend maken van informatie over leerlingen, deelnemers of studenten (bijv. de eigen website);
- het bekend maken van de activiteiten van de instelling of het instituut op de eigen website;
- het berekenen, vastleggen en innen van inschrijvingsgelden, school- en leskosten en bijdragen of vergoedingen;
- het behandelen van geschillen;
- het doen uitoefenen van accountantscontrole;
- de uitvoering of toepassing van een andere wet.

2. Dataminimalisatie

Gebruiken we die gegevens die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? Kunnen we met minder of bijvoorbeeld anonieme gegevens werken? Bewaren we de gegevens niet langer dan nodig?

3. Transparant

Hebben we de leerlingen of hun ouders vooraf helder geïnformeerd over het doel van de gegevensverwerking? Hebben we uitgelegd welke gegevens worden gebruikt en met wie deze worden gedeeld? Deze informatievoorziening vindt ongevraagd plaats.

4. Juistheid

Kloppen de persoonsgegevens die we gebruiken nog steeds? De persoonsgegevens moeten correct zijn en blijven.

5. Opslagbeperking

Bewaren we de gegevens niet te lang? Houden we ons aan de bewaartermijnen?

6. Integriteit en vertrouwelijkheid

Staan de gegevens op de juiste plaats en voor de juiste mensen beschikbaar? Hebben er niet te veel mensen toegang tot deze gegevens?

7. Verantwoordingsplicht

Kan de dataverantwoordelijke (bestuurder) aan deze regels voldoen? En kan de bestuurder dit aantonen?

Binnen Stroomm spreken we met elkaar af dat we altijd checken of we aan deze vuistregels voldoen bij het verzamelen en verstrekken van persoonsgegevens. Hiervoor gebruiken we onderstaand schema.

Zijn het persoonsgegevens?
Is er een grondslag voor verzamelen?
Doelbepaling Doelbinding → uitdrukkelijk omschreven
Dataminimalisatie → alleen wat nodig is voor het doel
Transparant → zijn betrokkenen geïnformeerd ?
Juistheid → zo nodig actualiseren
Opslagbeperking → bij voorkeur anoniem
Integriteit en vertrouwelijkheid → beveiliging
Verantwoordingsplicht → voldoe aan de AVG verplichting

Hoofdstuk 3 Privacyreglement en verklaring

Het privacyreglement is een document waarin nauwkeurig en op een begrijpelijke manier beschreven is welke persoonsgegevens binnen de organisatie worden verwerkt en met welk doel.

Ook is hierin te lezen wie toegang heeft tot deze gegevens, hoe de gegevens zijn beveiligd en met wie ze uitgewisseld mogen worden. Met het reglement voldoet het bestuur aan haar wettelijke informatieplicht, mits deze ook actief wordt aangeboden aan de ouders en medewerkers. Alle betrokkenen, zoals ouders en medewerkers, moeten daarom het privacyreglement kunnen inzien. Het privacyreglement is vastgesteld door de (G)MR.

Ouders moeten tijdens de aanmelding geïnformeerd worden over de gegevens die verzameld worden door de school en wat er met die gegevens gedaan wordt. Dit is opgenomen in de privacy verklaring/toelichting. De privacyverklaring is vastgesteld door de (G)MR.

Medewerkers en ouders kunnen het reglement en de verklaring inzien op de website www.stroomm.nl/avg. Op de sites van de scholen wordt verwezen naar dit adres zodat altijd de actuele informatie beschikbaar is.

Hoofdstuk 4 Toestemming foto's / video's en online diensten

Mobiele telefoon

Het gebruik van een mobiele telefoon binnen de school door leerlingen is sinds schooljaar 2024-2025 verboden.

Beeldmateriaal

Richtlijn voor het gebruik en toestemming beeldmateriaal

Privacy wordt in Nederland geregeld in de Algemene Verordening Gegevensbescherming (AVG). Foto's en video's van leerlingen zijn persoonsgegevens en vallen daarmee onder deze wet. Daarom gelden er aangescherpte eisen voor het gebruik van beeldmateriaal. Het gaat om alle vormen van gebruik, zoals:

- foto's die je als school in de nieuwsbrief plaatst;
- foto's die je deelt of op sociale media plaatst;
- een video die je vertoont op de website van de school.

De Autoriteit Persoonsgegevens (AP), is in Nederland toezichthouder op de uitvoering van de privacywetgeving. De AP heeft een aantal richtlijnen opgesteld voor het juist gebruik van beeldmateriaal op school.

Als een school foto's of video's van leerlingen gebruikt, dan is daar altijd toestemming van ouders voor nodig. Als de leerling 16 jaar of ouder is, moet de leerling daar zelf toestemming voor geven. Hierbij gelden de volgende voorwaarden:

- De toestemming moet in **vrijheid** worden gegeven. Hiermee wordt bedoeld dat ouders en leerlingen altijd moeten kunnen weigeren, zonder dat daar sancties aan zijn verbonden.

- De inschrijving van een leerling op school mag bijvoorbeeld niet afhankelijk zijn van de toestemming om beeldmateriaal te gebruiken.
- De toestemming moet **'ondubbelzinnig zijn'**. Dit betekent dat toestemming altijd nodig is. Als er geen reactie is op je vraag mag je niet aannemen dat de ouders het goed vinden dat je beeldmateriaal gebruikt. Wie zwijgt, stemt dus niet toe. Ook mag je de toestemming niet verbergen in de voorwaarden bij inschrijving of in de schoolregels. Je moet de toestemming namelijk altijd kunnen aantonen.
- De toestemming is **specifiek**. Dit houdt in dat het duidelijk is voor de leerling en zijn ouders waar toestemming voor wordt gegeven. Bij het vragen van toestemming is duidelijk hoe het beeldmateriaal wordt gebruikt: bijvoorbeeld op de website, nieuwsbrief of sociale media), en wat het doel is (bijvoorbeeld informeren van de ouders en leerlingen of promotie van de school).
- Toestemming die eenmaal is gegeven, **mag op ieder moment worden ingetrokken**. En natuurlijk gebruik je het beeldmateriaal niet als er (nog) geen toestemming is gegeven.

De beleidsregels van de AP benadrukken dat scholen het vragen om toestemming serieus moeten nemen. Ook al leidt dat tot extra administratieve rompslomp. Ten minste jaarlijks zal gewezen moeten worden op de toestemming die wel of niet is gegeven. Door het hele jaar heen moet het mogelijk zijn de toestemmingen aan te passen.

Stroomm voorziet via ParnasSys in de online-registratie van de toestemmingen.

Ouders/verzorgers kunnen het hele jaar terecht om hun voorkeur in te zien of eventueel aan te passen. Op deze manier krijgen medewerkers gelegenheid eventueel een toestemming te toetsen.

N.B.: Alle hierboven genoemde regels gelden ook voor de relatie school en medewerker.

Fotograferen van ouders

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) en zij moeten niet het risico lopen ongewenst gefotografeerd te worden.

Wanneer er activiteiten georganiseerd worden op een externe locatie, zoals bijvoorbeeld bij een excursie, sportdag of schoolreisje is het echter lastig om het maken van beeldopnames door ouders te verbieden.

Wij vragen daarom de ouders ook terughoudend te zijn met fotograferen en alleen hun eigen kinderen te fotograferen. Ook vragen wij ouders geen foto van andere leerlingen op hun eigen sociale media te plaatsen.

Online diensten

Voor het gebruik van online diensten door leerlingen binnen of buiten de school moeten ouders ook toestemming verlenen. Dit betekent dat wanneer leerlingen in de klas gebruik willen maken van een eigen (privé) account voor bijvoorbeeld Whatsapp of Pinterest, ouders hier vooraf toestemming voor moeten geven.

Dit betreft alleen online diensten die ook buiten de school om in het maatschappelijk verkeer gebruikt kunnen worden, dus niet voor e-mail, digitale leeromgevingen of leermiddelen waarvoor door de school zelf een account wordt verstrekt. Hiervoor heeft de school een verwerkersovereenkomst.

Hoofdstuk 5 Rechten van betrokkenen en klachten over privacy

Het is belangrijk om 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.

Hiervoor hebben we een procedure opgesteld.

Het verzoek komt doorgaans binnen bij de leerkracht. Deze speelt het verzoek direct door aan de directeur. De directeur neemt het verzoek in behandeling. Bij vragen kan de directeur terecht bij de Functionaris voor Gegevensbescherming (FG).

Betrokkenen kunnen een verzoek indienen bij de school of bij de verwerkingsverantwoordelijke (schoolbestuur).

Betrokkenen kunnen verzoeken doen, die zijn gebaseerd op de volgende rechten:

1. Recht op informatie
2. Recht op inzage in de gegevens
3. Recht op kopie van de gegevens
4. Recht op correctie en aanvulling (rectificatie)
5. Recht op vergetelheid (wissen van gegevens)
6. Recht om gegevens over te (laten) dragen (dataportibiliteit)
7. Recht op beperking van de verwerking
8. Recht om bezwaar te maken tegen de verwerking van gegevens

Als je zelf inzage wilt hebben in de gegevens die over jou zijn verzameld of je krijgt de vraag van een leerling of een ouder, dan kan dat op de volgende manier:

- Als medewerker kun je jouw vraag stellen aan de directeur.
- Een ouder of ander gezaghebbende die jou deze vraag stelt, verwijst je door naar de directeur (zie **Bijlage 2** Procedure rechten van betrokkenen).

In alle gevallen kan er ook altijd rechtstreeks contact opgenomen worden met de Functionaris voor Gegevensbescherming. De contactgegevens staan op de website.

Voor de directeuren is de uitgebreide procedure rechten van betrokkenen beschikbaar (**Bijlage 2**

Procedure rechten van betrokkenen). Een overzicht van welke ouder recht heeft op welke informatie (gezag kwesties) (**Bijlage 2a** Inzage tabel). Tevens is er voor de directeuren een registratieformulier beschikbaar om de genomen stappen te bewaken en aantoonbaar te maken (**Bijlage 2b** Genomen stappen rechten van betrokkenen).

Hoofdstuk 6 Functionaris voor Gegevensbescherming

Een Functionaris voor Gegevensbescherming (FG) is iemand die controleert of een school zich aan de regels van de Algemene Verordening Gegevensbescherming (AVG) houdt. Een schoolbestuur is verplicht een FG aan te wijzen. Scholen of vestigingen die onder een schoolbestuur vallen hoeven geen eigen FG aan te wijzen.

Naast een controlerende taak beoordeelt een FG beveiligingsincidenten en datalekken, adviseert het bestuur en maakt medewerkers bewust van het belang van informatiebeveiliging en privacy. De FG is dé vraagbaak als het gaat om verwerking van persoonsgegevens.

Daarnaast is de FG de contactpersoon voor de externe toezichthouder: de Autoriteit Persoonsgegevens. Binnen Stroomm hebben wij een Functionaris voor Gegevensbescherming aangesteld in de persoon van Ger Simjouw, g.simjouw@cedgroep.nl. In basis lopen alle vragen via onze interne Security Officer die bereikbaar is via privacy@stroomm.nl.

Het is ook mogelijk indien gewenst om rechtstreeks contact op te nemen met de Functionaris voor Gegevensbescherming. De regeling taken en verantwoordelijkheden Functionaris voor Gegevensbescherming zijn met instemming van de GMR vastgesteld en op te vragen bij het bestuur.

Hoofdstuk 7 Verwerkersovereenkomsten en verwerkersregister

Wat is een verwerkersovereenkomst?

In de nieuwe privacywet is bepaald dat de school afspraken moet maken met alle leveranciers van de school die leerlinggegevens verwerken in zogenaamde Verwerkersovereenkomsten. Het gaat bijvoorbeeld om uitgevers van digitaal lesmateriaal, leveranciers van toetsen, onderwijsadviesdiensten, etc.

Het belangrijkste hierbij is dat scholen, als gegevensverantwoordelijke, de regie hebben en houden over wat er gebeurt met de persoonsgegevens. Dit mag je niet overlaten aan de leverancier (verwerker). De school beslist wat de leverancier wél en niet met de gegevens mag doen.

Uitwisseling van gegevens met samenwerkingsverband

Een uitzondering hierop is de uitwisseling van gegevens met het samenwerkingsverband in het kader van passend onderwijs. Het samenwerkingsverband is een zelfstandige organisatie die zelf verantwoordelijk is voor de gegevens van leerlingen. De wet regelt dat een school gegevens uitwisselt met het samenwerkingsverband. Hiervoor hoeft daarom geen verwerkersovereenkomst afgesloten te worden. Het blijft natuurlijk wel belangrijk om de gegevens op de juiste manier uit te wisselen (zie

Hoofdstuk 11 Uitwisselen van gegevens).

Het afsluiten van een verwerkersovereenkomst

De verwerkersovereenkomsten worden bovenschools afgesloten. Wanneer een school een contract afsluit met een nieuwe leverancier zal er een nieuwe verwerkersovereenkomst gesloten moeten worden. Voordat de school een nieuw contract afsluit neemt de school eerst contact op met de Security Officer. Deze kijkt of het bestuur al een contract met deze leverancier heeft en zorgt anders eerst voor de verwerkersovereenkomst alvorens de school kan starten met de software. De privacy bijsluiters (deze zijn toegevoegd als bijlage bij een verwerkersovereenkomst) moeten inzichtelijk zijn voor ouders indien zij hierom vragen. Dit kan opgevraagd worden via privacy@stroomm.nl.

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

Verwerkersregister

Iedere verwerkingsverantwoordelijke moet een register van de verwerkingsactiviteiten die onder de verantwoordelijkheid van de verwerkingsverantwoordelijke vallen, in een register bijhouden (art. 30 AVG).

Het bestuur houdt de volgende gegevens in het register bij:

- de naam en de contactgegevens van de verwerkingsverantwoordelijke(n) en de functionaris voor gegevensbescherming;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen (Van wie worden persoonsgegevens verwerkt? Bijvoorbeeld leerlingen, ouders, medewerkers, oud-medewerkers);
- een beschrijving van de categorieën van persoonsgegevens (Wat voor persoonsgegevens worden er verwerkt? Bijvoorbeeld BSN, financiële gegevens etc.);
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- doorgiften van persoonsgegevens aan een derde land of internationale organisatie (indien van toepassing);
- indien mogelijk een algemene beschrijving van de technische en organisatorische maatregelen die genomen zijn om te beveiligen.

Wanneer er een nieuwe verwerking plaatsvindt, moet deze in het register komen te staan.

Het register en de verwerkersovereenkomsten zijn in te zien via het bestuur.

Hoofdstuk 8 Procedure datalekken

We spreken van een datalek wanneer er mogelijk 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.

Voorbeelden van datalekken zijn:

- een e-mail die aan een verkeerd persoon geadresseerd is
- verlies of diefstal van waardepapier, dossier, usb-stick, tablet of andere gegevensdragers, of inloggegevens die openbaar zijn geworden
- een gestolen telefoon
- een gehackte computer
- een phishing mail

Is er mogelijk sprake van een datalek, dan ben je als medewerker verplicht dit zo snel mogelijk te melden bij de Security Officer van Stroomm en bij je direct leidinggevende (ook als je twijfelt). Je kunt hiervoor het volgende emailadres gebruiken: privacy@stroomm.nl. Als er persoonsgegevens verloren, beschadigd of onrechtmatig ingezien zijn, dan moet er mogelijk binnen 72 uur een melding gedaan worden bij de Autoriteit Persoonsgegevens. De FG doet de melding in overleg met de verwerkingsverantwoordelijke.

Het bestuur van de school (bevoegd gezag) is verwerkingsverantwoordelijk 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 boete opgelegd worden aan het bestuur (bevoegd gezag).

In **Bijlage 3** Stappenplan datalekken is het stappenplan van de procedure datalekken opgenomen. Het volledige schema procedure melden datalekken is op te vragen bij het bestuur.

Hoofdstuk 9 Toegangsbeleid

Binnen de organisatie zijn veel persoonsgegevens aanwezig. Zowel van medewerkers als van leerlingen. Niet alle medewerkers hebben toegang nodig tot alle leerlinggegevens. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat iemand in 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.

Een leerkracht krijgt de toegang tot zijn/ haar eigen groep. Daarbij heeft de leerkracht de mogelijkheid tijdelijke toegang te vragen, dit wordt door het systeem direct verleend. De leerkracht moet hiervoor wel de reden voor de toegang invullen. Dit wordt gelogd.

De directeur van de school is verantwoordelijk voor het verstrekken van de juiste toegang (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 gecontroleerd.

De toegang tot gegevens van de medewerkers is beperkt tot de direct leidinggevende en diens vervanger en de HR afdeling van het bestuur. In **Bijlage 4** Toegangsmatrix vind je de toegangsmatrix.

Hoofdstuk 10 Gedragscode

Voor een veilig schoolklimaat is het belangrijk dat de afspraken rondom informatiebeveiliging en privacy door alle werknemers worden nageleefd en uitgedragen. Daarom is er een Gedragscode ICT en Internet opgesteld waaraan alle medewerkers van Stroomm zich dienen te houden.

De Gedragscode ICT en Internet is vastgesteld door de GMR en op te vragen bij privacy@stroomm.nl. Een exemplaar is ook aanwezig bij de directeur op de school.

Hoofdstuk 11 Uitwisselen van gegevens

Om ervoor te zorgen dat we binnen de school gegevens op de juiste wijze uitgewisseld worden hebben we een schema gemaakt wanneer er toestemming gevraagd moet worden en hoe de gegevens uitgewisseld worden.

In deze tabel staat met wie je gegevens uit mag wisselen en op welke wijze. Staat jouw doel er niet bij informeer dan altijd even bij de Functionaris voor Gegevensbescherming (FG).

Persoonsgegevens-verstrekken aan:	Het doel is:	Heb je toestemming nodig?
Overstap van PO naar andere basis-, SO/SBO of VO school	Overdracht (OKR,) leerlingendossier (na aanmelding) W	NEE maar ouders hebben wel inzage en de mogelijkheid hun zienswijze toe te voegen.
Overstap van VO naar VSO of andere VO school	Overdracht (OKR,) leerlingdossier (na aanmelding) W	JA ouders mogen bezwaar maken tegen deze uitwisseling. Ze moeten inzage gehad hebben en toestemming gegeven.
Dienst Uitvoering Onderwijs (DUO)	Bekostiging W	NEE
Inspectie van het Onderwijs	Toezicht W	NEE
Leerplicht gemeente	Controle verzuim W*	NEE
Administratiekantoor	Salarisadministratie en HRM	NEE , wel verwerkersovereenkomst
Samenwerkingsverband (SWV)	Advies, arrangement, Toelaatbaarheids-verklaring (TLV) (gegevens uit OPP) W	NEE , wel ouders informeren, géén BSN uitwisselen
Samenwerkingsverband (SWV)	Aanvullende gegevens op de OPP, voor TLV of advies of arrangement Bijv. onderzoekverslagen of informatie thuissituatie voor inzet jeugdhulp.	JA , voor alle medische verslagen is toestemming van de ouders nodig!
Samenwerkingsverband (SWV)	Thuiszitters tegengaan W	NEE
Educatieve uitgeverijen, Basispoort, Entree Federatie	Gebruik digitale middelen	NEE , wel verwerkersovereenkomsten met uitgeverijen
Educatieve apps (niet in beheer van de leerkracht of ICT)	Ondersteuning Onderwijs	JA , dit geldt als ze nadat de leerling school verlaten heeft de app nog gebruikt kan worden.
Externe onderwijs specialisten	Zorgbegeleiding (onderzoeken)	JA
Stagiaires (gegevens)	Opleiding	NEE , wel stage overeenkomst

Stagiaires (foto's/video/geluidsmateriaal)	Opleiding	NEE indien het materiaal binnen de school (Stroomm) blijft. JA indien het materiaal buiten de school gebruikt wordt – bijvoorbeeld als materiaal voor de eigen opleiding/stageopdrachten wordt gebruikt.
TSO/BSO	Tussenschoolse opvang, Buitenschoolse opvang	JA
GGD/JGZ*	Er mag niet uitgewisseld worden door de school!	n.v.t.*

W = Wettelijk verplicht

W*= Wettelijk verplicht en uitbesteed bij gemeente

* De GGD wisselt uit met DUO. Op dit moment werkt de uitwisseling via DUO nog niet overal goed. Indien de vraag toch komt, kun je overleggen met de FG.

Deze tabel is niet uitputtend. Staat het type persoonsgegevensverstrekking er niet bij, vraag dit dan na bij de Functionaris voor Gegevensbescherming (FG).

Hoofdstuk 12 Richtlijnen veilig mailen

E-mail is niet een bijzonder veilig medium. Mail kan onderweg onderschept worden. Je mailaccount kan natuurlijk gehackt worden, maar dat is iets dat ook bij andere uitwisselmedia kan gebeuren. Zeker zo belangrijk is dat een e-mail per ongeluk bij de verkeerde persoon terecht kan komen. Om daar de nadelige gevolgen van te voorkomen, kun je een aantal maatregelen treffen.

- 1. Check altijd of je inderdaad het goede e-mailadres ingevuld hebt.**
Let dus op wanneer je e-mailprogramma een adres automatisch aanvult.
- 2. Vul het e-mailadres pas op het laatst in, nadat je je bericht geschreven hebt.**
Dan kan de mail niet per ongeluk verstuurd worden.
- 3. Neem in je e-mailbericht niet meer informatie op dan noodzakelijk is.**
Persoonsgegevens mogen namelijk niet bij de verkeerde persoon terecht komen. Om toe te lichten wat je wel en wat je beter niet in je mail opneemt, zie je hieronder twee voorbeelden.

Voorbeeld 1

Leerkracht mailt aan andere leerkracht:

'Daan Verstraete gaat morgen niet mee zwemmen omdat hij oorontsteking heeft.'

Zowel de volledige naam als de vermelding van medische informatie zijn persoonsgegevens waarmee je zorgvuldig moet omgaan. Het is daarom beter dit bericht als volgt te formuleren:

'Daan gaat morgen niet mee zwemmen.'

In bijna alle gevallen weten de betrokkenen wel om welke Daan het gaat en de reden is minder belangrijk. Is de reden wel belangrijk, of is het noodzakelijk om andere persoonsgegevens te vermelden, mail dan beveiligd. Hiervoor is Zivver beschikbaar gesteld binnen alle scholen.

Voorbeeld 2

Leraar mailt aan ouder:

'De afgesproken intelligentietest bij uw dochter Hilde Özgül zal afgenomen worden op woensdag 5 oktober om 13.30 uur.'

Ook hier bevat de mail persoonsgegevens die niet in verkeerde handen terecht mogen komen. Een betere mail is daarom:

'De afgesproken test bij uw kind zal afgenomen worden op woensdag 5 oktober om 13.30 uur.'

Binnen Stroomm werken we met Office 365, hiermee is het mogelijk versleuteld te mailen (gebruik hiervoor Zivver). Via de ICT coördinator van de school is er een handleiding hiervoor beschikbaar.

Hoofdstuk 13 Bewaartermijnen

Archivering: bewaartermijnen

Door Kennisnet is - in samenspraak met het ministerie van OC&W - gekeken naar bewaartermijnen van persoonsgegevens. Naar aanleiding van het bewaartermijnenoverzicht dat door Kennisnet is opgesteld houden we onderstaande bewaartermijnen aan binnen Stroomm.

Dit zijn de vastgestelde bewaartermijnen onderwijs:

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Afwijkende bewaartermijn
Gegevens over in- en uitschrijving	5 jaar + 8 weken	datum van uitschrijving	
Gegevens over verzuim en afwezigheid	minimaal 5 jaar + 8 weken	datum van uitschrijving	
Gegevens die nodig zijn om de bekostiging te berekenen	minimaal 7 jaar	na afloop van het schooljaar waarop de bekostiging betrekking heeft	
Gegevens leerling na overstap naar speciaal onderwijs	3 jaar	Datum van uitschrijving	5 jaar*
Camera en videobeelden	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten	moment van opname	
Het onderwijskundig dossier	maximaal 2 jaar	datum van uitschrijving	5 jaar*
Gezondheidsgegevens die nodig zijn voor speciale begeleiding of voorzieningen	maximaal 2 jaar	datum van uitschrijving	5 jaar*

Adresgegevens	maximaal 2 jaar	datum van uitschrijving	5 jaar*
---------------	-----------------	-------------------------	---------

*I.v.m. de inspectie uitdraaien hanteren wij de afwijkende bewaartermijn van 5 jaar. Wij volgen hiermee het advies van Kennisnet en de PO/VO raad.

Indien de ouder hierom verzoekt kan er eerder verwijderd worden. Hiervoor is het verstandig dat de FG ingeschakeld worden.

Dit zijn de vastgestelde bewaartermijnen personeel:

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Afwijkende bewaartermijn
Sollicitatiebrieven, - formulieren, correspondentie omtrent de sollicitatie, getuigschriften	4 weken zonder toestemming, 1 jaar met toestemming van de sollicitant	na beëindiging sollicitatieprocedure	
VOG	1 jaar	einde dienstverband	5 jaar i.v.m. de accountantscontrole
Arbeidsovereenkomst en wijzigingen	2 jaar	einde dienstverband	
BSN	7 jaar	einde dienstverband	
Loonbelastingverklaringen en kopieën van identiteitsbewijzen	5 jaar	einde dienstverband	
Verslagen van functioneringsgesprekken	2 jaar	einde dienstverband	
Loonbeslagen	Tot opheffing	Tot opheffing	
Opleiding	5 jaar	einde dienstverband	
Personeelsdossier, Nationaliteit NAW, contactgegevens, geslacht, levensloop	7 jaar	einde dienstverband	
Correspondentie over benoemingen, promotie, demotie en ontslag	2 jaar	einde dienstverband	
Financiële gegevens salarisadministratie	7 jaar	einde dienstverband	

Hoofdstuk 14 Jaarplan privacy

Bij het bestuur en op elke school is een jaarplan aanwezig met punten die elk jaar aan de orde komen qua privacy. Denk hierbij aan verwijderen van leerlingendossiers en personeelsdossiers, het nakijken van de rechten, het wijzigen van de wachtwoorden etc.

Dit overzicht is in te zien via de directeur of op te vragen bij het bestuur.

Hoofdstuk 15 **Geheimhouding**

Voor alle medewerkers van Stroomm geldt een geheimhouding.

Zowel de werkgever als de werknemer nemen met betrekking tot hetgeen in of uit hoofde van hun functie vertrouwelijk te hunner kennis is genomen de nodige zorgvuldigheid en geheimhouding in acht. Dit geldt ook na beëindiging van het dienstverband. Ook met alle verwerkers is door middel van de verwerkersovereenkomst een geheimhouding afgesproken. Vrijwilligers op de scholen hebben een geheimhoudingsverklaring getekend. Dit formulier 'Geheimhoudingsverklaring' is op te vragen via privacy@stroomm.nl.

Hoofdstuk 16 **DPIA**

Met een DPIA brengen we de privacy risico's van een gegevensverwerking in kaart. Vervolgens kunnen we maatregelen treffen om deze risico's te verkleinen.

In de Nederlandse vertaling van de AVG wordt de term Data Protection Impact Assessment (DPIA) gegevensbeschermingseffectbeoordeling genoemd.

Wanneer een DPIA (Data Protection Impact Assessment)?

Een DPIA verplicht als een verwerking voldoet aan 2 of meer van de 9 criteria.

De 9 criteria zijn:

1. beoordelen van mensen op basis van persoonskenmerken;
2. geautomatiseerde beslissingen;
3. stelselmatige en grootschalige monitoring;
4. gevoelige gegevens;
5. grootschalige gegevensverwerkingen;
6. gekoppelde databases;
7. gegevens over kwetsbare personen (bijvoorbeeld kinderen);
8. gebruik van nieuwe technologieën;
9. blokkering van een recht, dienst of contract.

Ook als er aan slechts één - of geen - van deze criteria voldoet, moet er kunnen worden onderbouwd waarom er voor gekozen is om geen DPIA uit te voeren. Dit maakt onderdeel uit van de verantwoordingsplicht onder de AVG heeft. Bij een nieuwe verwerking wordt dus altijd gekeken of er een DPIA moet worden uitgevoerd.

Voor bestaande verwerkingen geldt dat er alleen een verplichting is om een DPIA uit te voeren als er iets verandert aan het risico van de gegevensverwerking. En de gegevensverwerking vervolgens (na de verandering) een hoog privacy risico oplevert.

Hoofdstuk 17 **Cameratoezicht**

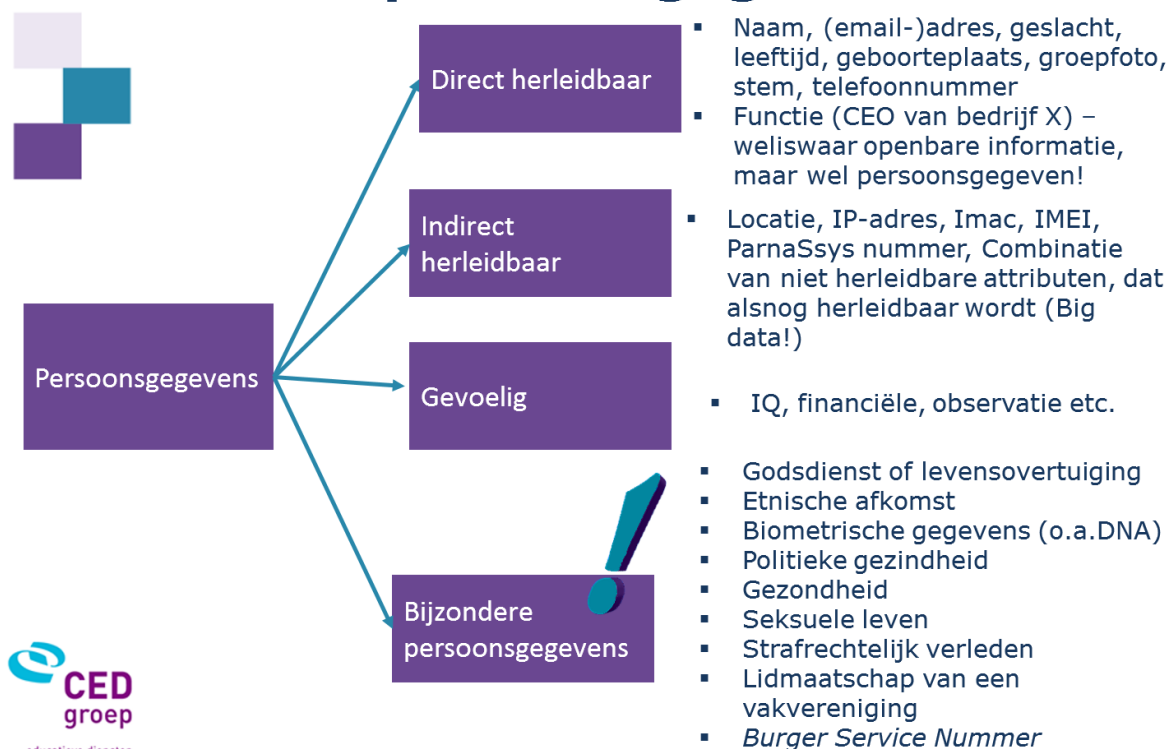
Van toepassing op obs De Spelwert, obs De Walsprong en obs De Tweestromenschool. Over het gebruik van cameratoezicht op de scholen is een apart protocol. Deze is met instemming van de GMR vastgesteld. Hierin te lezen valt waarom er in bepaalde gevallen gekozen kan worden voor cameratoezicht en welke afspraken daarover zijn.

Bijlagen

Bijlage 1	Persoonsgegevens
Bijlage 2	Procedure rechten van betrokkenen
Bijlage 2a	Inzage tabel
Bijlage 2b	Genomen stappen rechten van betrokken
Bijlage 3	Protocol datalekken
Bijlage 4	Toegangsmatrix

Bijlage 1 Persoonsgegevens

Wat is een persoonsgegeven?



Bijlage 2 Procedure rechten van betrokkenen

Procedure binnen de school

Wie behandelt een verzoek?

Het verzoek komt doorgaans binnen bij de leerkracht. Deze speelt het verzoek direct door aan de directeur. De directeur neemt het verzoek in behandeling.

Beoordeling van het verzoek

Beoordeel wat voor soort verzoek het is. Dit gebeurt door de directeur van de school of diens vervanger. Gaat het alleen om inzage, of ook om rectificatie, aanvulling, verwijdering of een beperking van de verwerking? Betrokkenen kunnen soms andere termen gebruiken, dus wees hier alert op. Afhankelijk van het soort verzoek moeten andere acties ondernomen worden. Denk hierbij aan het inschakelen van de functionaris voor Gegevensbescherming.

Betrokkenen kunnen een verzoek indienen bij de school of bij de verwerkingsverantwoordelijke (schoolbestuur).

Betrokkenen kunnen verzoeken doen, die zijn gebaseerd op de volgende rechten:

1. Recht op informatie
2. Recht op inzage in de gegevens
3. Recht op kopie van de gegevens
4. Recht op correctie en aanvulling (rectificatie)
5. Recht op vergetelheid (wissen van gegevens)
6. Recht om gegevens over te (laten) dragen (dataportibiliteit)
7. Recht op beperking van de verwerking
8. Recht om bezwaar te maken tegen de verwerking van gegevens

Voer een identiteitscontrole uit

Controleer de identiteit van de aanvrager voordat het verzoek verder in behandeling genomen wordt. Deze check moet zwaarder zijn naarmate het om meer gevoelige of zelfs bijzondere gegevens gaat. Voorkomen moet worden dat er een 'fake'-inzageverzoek gedaan wordt om zo gegevens te verzamelen. De controle kan al plaats gevonden hebben door de leerkracht als het verzoek bijvoorbeeld mondeling is binnen gekomen. De leerkracht heeft doorgaans contact met de ouder en kan een face to face verzoek controleren. Controleer of de verzoeker het gezag heeft. Ook een ouder zonder gezag heeft recht op informatie (Art. 1:377 b en c BW)¹

Indien de identiteit niet direct kan worden vastgesteld, registreer dan wanneer en welke vragen er gesteld zijn om de identiteit vast te stellen. Overleg eventueel met de Functionaris voor Gegevensbescherming.

¹ Het Burgerlijk Wetboek bepaalt dat de school verplicht is een ouder die niet het ouderlijk gezag heeft, als hij of zij daarom vraagt, van beroepshalve beschikbare informatie te voorzien over belangrijke feiten en omstandigheden die het kind of de verzorging en opvoeding van het kind betreffen. Er zijn op deze regel twee uitzonderingen:

- de informatie wordt niet verstrekt als de school de informatie niet op dezelfde manier aan de ouder met het ouderlijk gezag zou verstrekken;
- de informatie wordt niet verstrekt als het belang van het kind zich daartegen verzet.

Behandel het verzoek

De directeur houdt toezicht op de termijn waarin het verzoek afgehandeld moet worden. De directeur geeft aan wie het verzoek afhandelt. Dit kan de leerkracht zijn, de IB'er of de directeur zelf.

De directeur bepaalt of de Functionaris voor Gegevensbescherming wordt geraadpleegd of ingeschakeld.

Verwerk verzoek (anoniem) in register

Alle verzoeken die binnen een kalenderjaar geweest zijn worden door de directeur vastgelegd. Dit gebeurt in een klein overzicht waarin de volgende gegevens worden opgenomen:

- datum van afhandeling;
- omschrijving van het verzoek;
- door wie het is afgehandeld;
- of de Functionaris voor Gegevensbescherming er bij betrokken is.
- eventuele bijzonderheden.

In het register worden geen gegevens opgenomen die herleidbaar zijn naar een persoon.

Bijlage 2a Inzage tabel

Welke ouder heeft recht op welke informatie?

Hieronder vindt u een schema waarin de soorten verbintenissen tussen ouders zijn omschreven. Je kunt zo gemakkelijk zien welke ouder recht heeft op welke informatie.

	Voor wie	Alle informatie	Beperkte informatie (erkend)
A	Ouders die met elkaar zijn getrouwd; voor vader en moeder geldt:	X	
B	Ouders die zijn gescheiden; Voor vader en moeder geldt:	X N.B. geen informatie geven die mogelijk gebruikt kan worden om voordeel ten koste van de andere ouder te behalen	
C	Ouders die hun partnerschap hebben laten registreren	X	
D	Ouders die niet met elkaar zijn getrouwd, maar via goedkeuring van de rechtbank het gezamenlijk gezag uitoefenen	X	
E	Ouder die niet met het gezag is belast		X artikel 1:377c BW
F	In geval van samenwonen, vader heeft kind erkend, niet ingeschreven in gezagsregister; voor vader geldt:		X artikel 1:377c BW
G	In geval van samenwonen, vader heeft kind erkend en ingeschreven in gezagsregister; voor vader en moeder geldt:	X	
H	Stel heeft samengewoond, nu uit elkaar, kind is erkend, ingeschreven in gezagsregister; voor vader en moeder geldt:	X N.B. geen informatie geven die mogelijk gebruikt kan worden om voordeel ten koste van de andere ouder te behalen	
I	Stel heeft samengewoond, nu uit elkaar, kind is erkend, maar niet ingeschreven in het gezagsregister; voor vader geldt:		X artikel 1:377c BW
J	Ouders beide uit de ouderlijke macht gezet, kind is onder voogdij geplaatst; voor vader en moeder geldt:		X artikel 1:377c BW
K	Voogd	X	
L	Biologische vader, die zijn kind niet heeft erkend		
M	Grootouders die de verzorging van het kind op zich nemen omdat de ouders spoorloos zijn.		

L: Voor de biologische vader, die zijn kind niet heeft erkend, geldt dus: helemaal geen informatie.

M: Voor grootouders, die de verzorging van de kinderen op zich nemen, omdat de ouders spoorloos zijn geldt: **in principe geen** informatie.

Bijlage 2b **Genomen stappen rechten van betrokkenen**

Rechten van betrokken genomen stappen

- Verzoek
- ☐ Inzage
 - ☐ Copy
 - ☐ Correctie
 - ☐ Aanvulling
 - ☐ Mening toevoegen
 - ☐ Overdracht
 - ☐ Wijziging
 - ☐ Vernietiging
 - ☐ Beperking

Betreft leerling dossiernummer:

Intern nummer:

Stap/vraag	Datum	Omschrijving / vraag	Uitgevoerd door
Ontvangst verzoek			
Controle identiteit*			
Overleg leerkracht/ bestuurder /			
Verzoek behandelen			
Overleg FG			

Controle identiteit kan bijvoorbeeld als er een verzoek binnen is gekomen per mail; check uitvoeren of dit mail adres bekend is in het LAS systeem.

In sommige gevallen (bij verzoeken om bijzondere persoonsgegevens) kan controle door middel van ID wenselijk zijn.

FG inschakelen bij complexe zaken.

Bijlage 3 Stappenplan datalekken

	Procedurestap	Termijn	Wie
1	Beveiligingsincident • Verlies USB stick • Verlies iPad, smartphone, laptop • Verzending naar verkeerd mailadres • Verlies dossier • Onbevoegde die toegang had tot netwerk of bestand • Phishing • Hacking		Ontdekker lek
1	Beveiligingsincident melden bij direct leidinggevende en Security Officer via privacy@stroomm.nl .	Direct	Ontdekker lek
1a	Indien telefoon verloren etc. direct gaan blokkeren (ook privé telefoon)	Direct	Ontdekker lek / Security Officer
1b	Ook persoonsgegevens gelekt? Dan ook melden bij functionaris gegevensbescherming (FG) Ger Simjouw , g.simjouw@cedgroep.nl	Direct	Ontdekker lek / Security Officer/ Directeur
2	In behandeling nemen beveiligingsincident	Direct	FG
3	Maatregelen treffen om datalek te stoppen	Direct	Security Officer i.o.m. FG
3a	Informeren bestuurder over datalek	Direct	Security Officer
4	Beoordelen of er sprake is van een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) 1. Of er sprake is van een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) 2. Of betrokkene(n) wiens gegevens gelekt zijn geïnformeerd moet(en) worden 3. Of er actie ondernomen moet worden naar derden: • Informatie • Maatregelen • Onderzoek 4. Of de RvT e/o GMR geïnformeerd moeten worden 5. Of externe communicatie nodig is	Binnen 72 uur na ontdekken van lek	FG in overleg met: • Medewerker /Directeur • Direct leidinggevende • Bestuurder
5	Informeren bestuurder over stand van zaken en beoordeling	Binnen 72 uur	FG
6	Bij meldingsplichtig datalek: melden bij AP via meldloket: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0	Binnen 72 uur	FG i.o.m bestuurder
7	Als betrokkene(n) wiens gegevens gelekt zijn geïnformeerd moet(en) worden, versturen kennisgeving met vermelding van: • Aard inbreuk • Contactgegevens • De maatregelen die betrokkene kan nemen om negatieve gevolgen te beperken Afhankelijk van de omvang van het datalek overwegen om andere kanalen in te zetten.	Zo snel mogelijk, uiterlijk binnen 72 uur	FG in overleg met medewerker / directeur dat gegevens verwerkt FG in overleg met bestuurder
7a	Externe communicatie (indien nodig)	Zo snel mogelijk	Bestuurder/ directeur /FG en PR/communicatie
7b	Controle op effectiviteit van de afhandeling van incidenten en datalekken per kwartaal	FG	Per kwartaal
7c	Jaarlijkse rapportage over aantal datalekken aan RvT en GMR	Per jaar	FG iom bestuurder

Bijlage 4 Toegangsmatrix

Rollen en rechten ParnasSys

Functies/rollen	Rol in ParnasSys ¹	Werkzaamheden	Niveau van toegang ¹ :
Bovenschools			
Bestuurder	Monitororganisatie beheerder	Sturing en beleid	Stichting
Directie(raad)	Monitororganisatie beheerder	Sturing en beleid	Stichting
School			
Leerkrachten	Leerkracht	Verzorgen onderwijs	Groep en parallel
Invalleerkracht	Leerkracht	Verzorgen onderwijs	Groep
Invalleerkracht kort	Leerkracht	Verzorgen onderwijs	Groep/Invallersaccount
LIO-stagiaire	Leerkracht (voor periode blok)	Verzorgen onderwijs	Groep
Directeur	Applicatiebeheerder	Sturing en beleid	School
Intern begeleider	Intern begeleider	Leerlingzorg	School
Orthopedagoog	Intern begeleider	Leerlingzorg	School
School-maatschappelijk werk	Intern begeleider	Leerlingzorg	School
Logopedist	Intern begeleider	Leerlingzorg	School
Ondersteuner (arrangementen enz.)	Leerkracht	Verzorgen onderwijs	School/Subgroep
Administratief medewerker	Administratie / leerkracht ³	Administratietaken	School
Extra rollen op schoolniveau			
Beheerder ParnasSys ⁴	Applicatiebeheerder	Beheer	School

¹ Zie hier onder voor toegangsrechten die standaard per rol zijn ingesteld in ParnasSys

² De volgende toegangsniveaus worden onderscheiden:

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

³ Indien administratief medewerkers aanmeldformulieren en overdrachtsdocumenten van het kinderdagverblijf moeten invoeren, moeten zij ook de rol leerkracht hebben op groepsniveau.

⁴ Deze rol kan bij Directeur, IB'er of ICT'er belegd worden, afhankelijk van het taakbeleid van de school.

Tabblad Leerling

	Leerling	Groep	Medewerker	School	Overzichten	Beheer	Mijn PamasSys		
Subtab	Optie	Applicatiebeheerder	Administratie	Intern Begeleider	Leerkracht	Leerkracht beperkt	Accountbeheerder		
Leerlingkaart		I	I	I	I	I	-		
Personalia	Personalia	X	X	I	I	I	-		
	Gezin	X	X	I	I	I	-		
	Medisch	X	X	X	X	I	-		
	BRON	X	X	-	-	-	-		
Onderwijs	Voorgeschiedenis	X	X	X	-	-	-		
	Deze school	X	X	(X)	I	I	-		
	Speciaal onderwijs	X	X	X	-	-	-		
	Passend onderwijs	X	X	X	-	-	-		
	Vervolgonderwijs	X	X	-	-	-	-		
	Absentie	X	X	X	X	-	-		
	Overstapdossier klaarzetten	X	X	X	X	-	-		
	Overstapdossier opvragen	X	X	-	-	-	-		
Toetsen	Niet-methodetoetsen	X	-	X	X	I	-		
	Methodetoetsen	X	-	X	X	I	-		
	Rapporten	X	-	I	X	I	-		
	Eindtoetsen	X	X	-	-	-	-		
	Didactische leeftijd	X	-	X	-	-	-		
	Ontwikkelprognose	X	-	X	-	-	-		
	IQ-testen	X	-	X	X	-	-		
Begeleiding	Plannen	X	-	X	X	I	-		
	Zorgdossier	-	-	-	-	-	-		
	Ontwikkelingsperspectief	X	I	X	X	I	-		
	Onderwijskundig rapport	-	-	-	-	-	-		
	Observatielijsten	X	-	X	X	I	-		
Map	Documenten	X	-	X	(X)	(X)	-		
	E-mails	X	-	X	X	X	-		

Tabblad Groep

	Leerling	Groep	Medewerker	School	Overzichten	Beheer	Mijn PamasSys		
Subtab	Optie	Applicatiebeheerder	Administratie	Intern Begeleider	Leerkracht	Leerkracht beperkt	Accountbeheerder		
Overzicht		I	I	I	I	I	-		
Leerlingen	Jaarovergang	X	X	-	-	-	-		
	Sublesgroepoverzicht	I	-	I	I	I	-		
	Uitschrijven	X	X	-	-	-	-		
	Plattegrond	X	X	X	X	X	-		
Groepskaart		X	-	X	X	-	-		
Absentie	Invoer	X	X	X	X	-	-		
	Overzicht	X	X	X	X	-	-		
Rooster	Lesrooster	X	X	X	X	I	-		
	Leerkrachtrooster	X	X	-	X	X	-		
Toetsen	Niet-methodetoetsen	X	-	X	X	I	-		
	Methodetoetsen	X	-	X	X	I	-		
	Rapporten	X	-	I	X	I	-		
	IQ-testen	(X)	-	(X)	(X)	I	-		
Begeleiding	Groepsplannen	X	-	X	X	I	-		
	Plannen	X	-	X	X	I	-		
	Sociogrammen	X	-	X	X	I	-		
	Observatielijsten	X	-	X	X	(X)	-		
Map		X	-	X	(X)	I	-		

Tabblad Medewerker

	Leerling	Groep	Medewerker	School	Overzichten	Beheer	Mijn PamasSys		
Subtab	Optie	Applicatiebeheerder	Administratie	Intern Begeleider	Leerkracht	Leerkracht beperkt	Accountbeheerder		
Overzicht		I	I	I	I	I	I		
Personalia	Medewerker	X	-	-	-	-	X		
	Aanstelling	X	-	-	-	-	X		
Map		E	E	E	E	E	E		

Tabblad School

	Leerling	Groep	Medewerker	School	Overzichten	Beheer	Mijn PamasSys		
Subtab	Optie	Applicatiebeheerder	Administratie	Intern Begeleider	Leerkracht	Leerkracht beperkt	Accountbeheerder		
Jaarplan	Activiteiten	X	X	I	I	I	-		
	Kalender	X	X	I	I	I	-		
	Urenoverzicht groepen	X	X	-	-	-	-		
Import	Eindtoetsresultaten	X	X	-	-	-	-		
Export	EDEX	X	X	-	-	-	-		
	DOD (Digitaal Overdrachts Dossier)	X	X	-	-	-	-		
Bron	Verstuur leerling BRON berichten	X	X	-	-	-	-		
	Verstuur speciale BRON berichten	X	X	-	-	-	-		
	Verwerk BRON terugkoppelingen	X	X	-	-	-	-		
	Leerlingaantallen	X	X	-	-	-	-		
OSO	Certificaat en URL	X	X	-	-	-	-		
	Overstapdossiers klaarzetten	X	X	X	X	-	-		
	Overstapdossiers opvragen	X	X	-	-	-	-		
	Dossieraanvragen	X	X	-	-	-	-		
Gespreksplanner		X	X	-	-	-	-		
Map	E-mails	X	X	X	X	-	-		
	Facturen	X	X	-	(X)	-	-		
Controles		X	X	-	-	-	-		
Info		X	X	-	-	-	-		

	Leerling	Groep	Medewerker	School	Overzichten	Beheer	Mijn PamasSys		
Subtab	Rubriek	Optie	Applicatiebeheerder	Administratie	Intern Begeleider	Leerkracht	Leerkracht beperkt	Accountbeheerder	
Beheer	Algemeen	Briefhoofd	X	-	-	-	-	-	
		Beperkingen	X	-	-	-	-	-	
		Nevenvestigingen	X	-	-	-	-	-	
		Prullenbak	X	-	-	-	-	-	
		Relaties	X	X	-	-	-	-	
		Rubrieken	X	-	-	-	-	-	
		Schoolmededelingen	X	X	-	-	-	-	
		Verzorgers	X	X	-	-	-	-	
		Wachtwoordreken	X	X	-	-	-	-	
	Facturen	Algemeen features	X	-	-	-	-	-	
		Facturen	X	X	-	-	-	-	
		Facturatiegegevens	X	-	-	-	-	-	
	Schoottabellen	Absentieredienen	X	-	-	-	-	-	
		Activiteitscategoriën	X	X	-	-	-	-	
		Benoemingen	X	-	-	-	-	-	
		Dienstverbanden	X	-	-	-	-	-	
		Gezindtes	X	X	-	-	-	-	
		Huisartsen	X	X	-	-	-	-	
		Sociogramtellingparen	X	-	-	-	-	-	
	Koppelingen	Certificaten	X	X	-	-	-	-	
		Koppelingen	X	-	-	-	-	-	
		Pasfoto's uploaden	X	X	-	-	-	-	
	Toetsen en vakken	Eindtoetsgemiddelden	X	-	-	-	-	-	
		Methodetoetsen	X	-	X	-	-	-	
		Niet-methodetoetsen	X	-	X	-	-	-	
		Vakken	X	-	-	-	-	-	
	Digitaal rapport	Digitaal rapport	X	-	-	-	-	-	
		Rapport/lerschalen	X	-	-	-	-	-	
	Begeleiding	Ontwikkelingsperspectief	X	-	X	-	-	-	
		Planacategoriën leerling	X	-	X	-	-	-	
		Planacategoriën groep	X	-	X	-	-	-	
	Map	Bestandscategoriën leerling	X	-	X	-	-	-	
		Bestandscategoriën medewerker	X	-	X	-	-	-	
		Nottiecategoriën leerling	X	-	X	-	-	-	
		Nottiecategoriën medewerker	X	-	X	-	-	-	
	Vragenlijsten	Vragenlijstjablonen	X	-	-	-	-	-	
Release notes			I	I	I	I	I	I	

Toelichting rechtenstructuur

I	= inzien
X	= inzien / opvragen, toevoegen en wijzigen
(X)	= inzien / opvragen en deels toevoegen en wijzigen
E	= enkel eigen gegevens inzien / opvragen en wijzigen
-	= niet beschikbaar

Toegang andere groepen

Een leerkracht heeft toegang tot de eigen groep en eventueel de groepen waarin groepsdoorbroken gewerkt wordt (voorbeeld parallelgroepen). Een leerkracht kan tijdelijke (tot maximaal een week) toegang vragen tot andere groepen. Hiervoor moet de leerkracht een bericht invoeren waarom deze toegang nodig is. Dit kan bijvoorbeeld nodig zijn i.v.m. vervanging. Dit bericht wordt gelogd.

Toegangslogging

Toegangslogging betreft het vastleggen van activiteiten waarbij toegang tot leerling gegevens is verkregen. Het doel is achteraf te kunnen vaststellen welke inzage in dossiers er is geweest en door wie dat is gedaan. Het bijhouden van een toegangslog maakt het mogelijk om onterechte en ongewenste inzage aantoonbaar te maken en daar, weliswaar achteraf, actie op te ondernemen.

In ParnasSys staat de logging aan. Hier wordt minimaal 2x per jaar een controle op uitgevoerd. Deze logging wordt uitgedraaid door de directeur, en gecontroleerd op onregelmatigheden. Bij een constatering van onregelmatigheden maakt de directeur een melding bij de Security Officer via privacy@stroomm.nl. Deze momenten staan in de jaarplanning. De Functionaris houdt hier toezicht op. Bij incidenten zal er vaker naar de logbestanden gekeken worden. Elk mogelijk incident wordt voorgelegd aan de FG.

Ook kan er tussentijds soms binnen een week weer een nieuwe log plaatsvinden.

De logbestanden worden een half jaar bewaard. M.u.v. van de incidentenlog deze worden bewaard zolang het onderzoek alsmede de afhandeling loopt.

Rollen en rechten Office 365

Documenten die betrekking hebben op individuele leerlingen worden opgeslagen in ParnasSys.

Documenten die betrekking hebben op de groepen worden opgeslagen in de afgeschermdede teamsites, mappen of fotoalbums. Je kan dit ook in ParnasSys bewaren in de groep.

Er worden alleen foto's bewaard waar leerlingen op staan die toestemming hebben verstrekt.

Personeelsdocumenten worden opgeslagen in de personeelsdossiers in Afas/Cupella.

Toegang personeelsbestanden

De toegang tot personeelsbestanden is geregeld via functierollen. Leidinggevend, salarisadministratie, personeelsadministratie en bestuurder.

Papieren dossiers zijn niet meer aanwezig, of zitten in afgesloten kasten. Bij verlies van de sleutel wordt direct de bestuurder ingelicht. Deze onderzoekt of er eventueel sprake is van een mogelijk datalek en neemt passende maatregelen om ongewenste toegang te voorkomen.

De sleutel is persoonsgebonden en wordt nooit aan een ander afgegeven. Ook niet aan een collega die er gezien zijn functie in zou mogen.

Toegang gebouw

De toegang voor de gebouwen is geregeld via een alarm(code)/druppel en/of sleutel. Bij verlies van de sleutel, druppel of alarmcode wordt direct de directeur ingelicht.

De directeur onderzoekt of er eventueel sprake is van een mogelijk datalek en neemt passende maatregelen om ongewenste toegang te voorkomen.

De code/druppel/sleutel is persoonsgebonden en wordt nooit aan een ander afgegeven. Ook niet aan een collega.

Toegang gebouw gedurende de lessen

Tijdens de lessen zijn de gebouwen, indien mogelijk, alleen vanaf binnen te openen. Bezoekers moeten aanbellen.

Toegang serverruimte

De ruimte bestemd voor ICT-toepassingen is toegankelijk voor ICT en directie. Deze ruimte is gedurende de dag altijd afgesloten.

Bij verlies van de sleutel, druppel en of code wordt direct de directeur ingelicht. De directeur onderzoekt

of er eventueel sprake is van een mogelijk datalek en neemt passende maatregelen om ongewenste toegang te voorkomen.

De code/sleutel is persoonsgebonden en wordt nooit aan een ander afgegeven. Ook niet aan een collega.

Toegang ruimte/kast papieren dossiers

De dossiers bevinden zich in een afgesloten ruimte/kast. Hiertoe hebben alleen medewerkers toegang die deze gegevens nodig hebben bij het uitvoeren van hun werkzaamheden. Dossiers worden alleen bewaard in deze afgesloten ruimte/kast.

De ruimte/kast is gedurende de dag altijd afgesloten.

De code/druppel/sleutel is persoonsgebonden en wordt nooit aan een ander afgegeven. Ook niet aan een collega.

Bij verlies van de sleutel/druppel en of code wordt direct de directeur ingelicht. De directeur onderzoekt of er eventueel sprake is van een mogelijk datalek en neemt passende maatregelen om ongewenste toegang te voorkomen.

Toegang Wifi-netwerk

Er is een toegangscode voor de medewerker en voor gasten/leerlingen.

De toegangscode voor gasten/leerlingen is beschikbaar. Deze code wordt tenminste één maal per jaar gewijzigd, vóór de zomervakantie.

De toegangscode voor de medewerkers is beschikbaar. Deze code wordt één keer per jaar gewijzigd.

Toegang magazijn

Het magazijn is niet toegankelijk voor leerlingen en of ouders. Het magazijn kan open zijn gedurende de dag. Alle personeelsleden letten op of er geen onbevoegden in het magazijn komen. In het magazijn zijn geen persoonsgegevens aanwezig.

Toegang stagiaires

Stagiaires hebben toegang voor specifieke (onderwijs)software. Dit wordt door de directeur per stageopdracht beoordeeld en vastgelegd in de stageovereenkomst. Bij beëindiging van de stage wordt voor de stagiaire handmatig de toegang tot diverse software geblokkeerd. Dit wordt genoteerd en opgeslagen bij de documenten van de stagiaire.

Toegangscontrole

Jaarlijks worden alle toegangen opnieuw gecontroleerd en beoordeeld. Hiervan is een kort verslag aanwezig.

Alarmcodes worden jaarlijks opnieuw ingesteld indien het om één code gaat. Indien elke werknemer een eigen code heeft, is dit niet nodig.

Bij in / uitdienst worden de sleutels en of druppel uitgereikt of ingenomen. Hiervoor wordt getekend door de medewerker en directeur.

