Handboek Informatiebeveiliging en Privacy

fluvium
openbaar onderwijs

PRIVACY
OP SCHOOL

Inhoudsopgave

Inleiding

Informatie en ict zijn noodzakelijk in de uitvoering van het onderwijs. Omdat we 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 persoonsgegevens te beschermen. Hiervoor is er binnen het bestuur dit IBP-Handboek opgesteld.

Dit handboek is bedoeld om uitvoering te geven aan het IBP-beleidsplan. In het handboek staan richtlijnen, procedures, afspraken en praktische handreikingen die nodig zijn om informatiebeveiliging en privacy goed te regelen. Deze maatregelen nemen we niet alleen omdat de wet dit voorschrijft, maar ook op basis van de normen en waarden die wij vanuit onze visie op onderwijs met elkaar delen en uitdragen:

De scholen van Stichting Fluvium Openbaar Onderwijs maken actief werk van de veelkleurigheid die onze samenleving kenmerkt. Zij denken niet in 'hokjes' en dragen bij aan democratisch burgerschap. We gaan kinderen voor in het leren van elkaar en het respecteren van diverse culturele, levensbeschouwelijke en economische achtergronden. Wij sluiten niemand buiten.

Op basis van gelijkwaardigheid leren onze kinderen dat iedereen verschillend mag zijn. En dat we daarin blijvend van elkaar leren.

Het handboek is onderverdeeld in twee delen voor twee afzonderlijke doelgroepen:

Deel A - Alle medewerkers
Dit deel bevat de algemene informatie die voor alle medewerkers binnen het bestuur 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. In dit deel wordt o.a. antwoord gegeven op de volgende vragen:

- Waar moet ik op letten bij het **verzamelen of delen** van gegevens?
- Welke **afspraken** gelden er voor mij als het gaat om leerlinggegevens?
- **Welke gegevens** bewaart de school van mij en waarvoor?
- Waar moet ik op letten bij het gebruik van **foto's en video's**?
- Als ik gegevens **kwijt** ben of ik heb een vermoeden van **misbruik**, bij wie moet ik dan zijn?
- Waar moet ik persoonsgegevens of persoonlijke informatie **opslaan**?

Deel B – Directeur en leidinggevenden
In dit deel is informatie terug te vinden die vooral van belang is voor de directeur: hoe zorg ik ervoor dat het IBP-beleid op mijn school goed geregeld is? In dit deel wordt o.a. antwoord

gegeven op de volgende vragen:

- Wat moet ik met **ouders** regelen rondom privacy?
- Welke **afspraken** moet ik maken met mijn medewerkers in het kader van privacy?
- Wat moet ik weten over **datalekken**?
- Wat moet ik weten als het gaat om het **verlenen van toegang** tot persoonsgegevens?
- Hoe lang moet ik persoonsgegevens **bewaren**?
- Welke afspraken maak ik over devices die in **bruikleen** worden gebruikt?
- Wat moet ik weten over **externe partijen** die namens de school persoonsgegevens verwerken?
- Welke **rollen en verantwoordelijkheden** t.a.v. IBP zijn er binnen de schoolorganisatie belegd?
- Hoe kan ik aantonen dat ik IBP **op orde** heb?

Deel A

Informatie voor alle medewerkers

Deel A geeft antwoord op de volgende vragen

- Waar moet ik op letten bij het **verzamelen of delen** van gegevens?
- Welke **afspraken** gelden er voor mij als het gaat om leerlinggegevens?
- **Welke gegevens** bewaart de school van mij en waarvoor?
- Waar moet ik op letten bij het gebruik van **foto's en video's**?
- Als ik gegevens **kwijt** ben of ik heb een vermoeden van **misbruik**, bij wie moet ik dan zijn?
- Waar moet ik persoonsgegevens of persoonlijke informatie **opslaan**?

Vuistregels Privacy

Privacy is een lastig en vaag begrip. Privacy op school gaat over de bescherming van gegevens van leerlingen, hun ouders en medewerkers. Dit wordt geregeld in de Algemene Verordening Gegevensbescherming (voorheen de Wet Bescherming Persoonsgegevens).

Wat zijn persoonsgegevens?
Dit zijn 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. Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd.

Binnen ons bestuur 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 ons bestuur spreken we met elkaar af dat we altijd nagaan of we aan deze vuistregels voldoen bij het verzamelen en verstrekken van persoonsgegevens aan de hand van de volgende vragen. (Dit hoeft niet voor elke verwerking schriftelijk worden vastgelegd.)

c	**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?

c	**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 po/vo, 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. voor de tussenschoolse opvang (TSO) van kinderen; ● er sprake is van een gerechtvaardigd belang, zoals het goed laten werken van digitale leermiddelen. Bijv. voor Basispoort en educatieve uitgeverijen.
c	**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?
c	**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?
c	**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?

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 voor alle medewerkers een gedragscode opgesteld.

De afspraken zijn verdeeld in drie onderdelen:
A. Waar en hoe bewaar ik persoonsgegevens?
B. Hoe en wat communiceer ik online via e-mail en sociale media?
C. Hoe houd ik indringers op afstand?

Hieronder volgen per onderdeel de gedragsregels die voor iedereen gelden bij de verwerking van gegevens van zowel leerlingen, ouders als die van medewerkers.

A. Waar en hoe bewaar ik persoonsgegevens?

1. *Verwerk persoonsgegevens zoveel mogelijk digitaal in de daarvoor aangewezen bewaarplaatsen.*
   Leerlinggegevens worden zoveel mogelijk digitaal opgeslagen, geraadpleegd en bewerkt in het Leerling volgsysteem (ParnasSys). Dit geldt ook voor gegevens die via ouders en/of externen worden ontvangen.
   Personeelsgegevens worden zoveel mogelijk digitaal opgeslagen in het financiële administratiesysteem en HR-systeem. Er worden geen persoonsgegevens op USB-sticks bewaard.
   Gegevens die op papier aangeleverd worden, worden gescand en aan bovengenoemde systemen toegevoegd. De scan wordt ook van de printer verwijderd, deze actie is of wordt door de medewerker ICT geregeld. Geef aangeleverde documenten terug aan degene die het aangeleverd heeft of vernietig deze gegevens in de papierversnipperaar.

2. *Formuleer gegevens die je vastlegt over een persoon zorgvuldig en professioneel.* Ouders en medewerkers hebben het recht om hun dossier in te zien. Zorg ervoor dat de gegevens zodanig professioneel zijn geformuleerd dat dit kan.

3. *Wanneer je persoonsgegevens verwerkt maak je altijd gebruik van de beveiligde Google Drive omgeving. Je slaat dus <u>nooit</u> gegevens op op je eigen computer of device.*
   Kun je de gegevens niet rechtstreeks opslaan in de Drive, maar moet je ze eerst downloaden op je computer? Doe dit alleen op een beveiligde computer (die voorzien is van een wachtwoord en up-to-date antivirus). Zet de bestanden direct in de Drive en verwijder de gedownloade bestanden van je computer. Zorg ervoor dat anderen (bijv. familieleden) niet bij jouw werkbestanden kunnen komen.

4. *Ga na welke afspraken er binnen de school gemaakt zijn voordat je persoonsgegevens uitwisselt met derden.*
   Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een arbo- of schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en houd daarbij ook rekening met de verdeling van het ouderlijk gezag. Voor de uitwisseling van gegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Vraag de IB-er voor meer informatie hierover.

   Ook al vragen derden om de levering van persoonsgegevens, je bent niet altijd verplicht om ze te geven. Controleer bij het verzamelen of delen van persoonsgegevens of hiervoor een wettelijke grondslag bestaat aan de hand van de Vuistregels Privacy. Tip: Bekijk in het privacyreglement met welke partijen gegevens (mogen) worden uitgewisseld.

5. *Informeer derden (ouders, hupverleners etc.) wanneer je door hen aangeleverde informatie (zowel geschreven als mondeling) opslaat in het leerlingdossier.*
   Als er contact is met een externe hulpverlener, is er hiervoor vaak al toestemming gevraagd. Je hoeft dan niet voor elke uitwisseling opnieuw toestemming te vragen, maar bij het vastleggen van sommige gevoelige informatie is het goed om ouders of hulpverlener te informeren over wat je op gaat nemen in het dossier. Bijvoorbeeld wanneer je bijvoorbeeld telefonisch contact hebt over een leerling met een hulpverlener en je wilt die informatie opslaan in het leerlingdossier. Informeer dan zowel de hulpverlener als de ouders welke informatie je aan het dossier toevoegt.

B. Hoe en wat communiceer ik online?

1. *Maak gebruik van een link naar het digitaal administratiesysteem om persoonsgegevens uit te wisselen met collega's.*
   Verstuur persoonsgegevens bij voorkeur niet per mail, maar verstuur een link met de online bewaarplaats van de benodigde gegevens.

2. *Vraag ouders om toestemming om een (privé)account aan te maken voor online diensten.*
   Leerlingen (jonger dan 16 jaar) moeten toestemming hebben van hun ouders/verzorgers om een (privé)account aan te maken voor online diensten zoals Pinterest, Kahood, Canva, etc. Het Google account is in beheer van de school en is noodzakelijk voor de organisatie van het onderwijs. Daarom valt het Google account onder de grondslag 'gerechtvaardigd belang' in plaats van 'toestemming', er hoeft dus geen toestemming gevraagd te worden.

3. *Deel over leerlingen, ouders of collega's nooit informatie via social media.*
   Doe dit vooral in persoon of desnoods via de telefoon. Wat je communiceert via social media kan makkelijk anders worden geïnterpreteerd door de lezer als je hier niet alert op bent.

4. *Deel alleen kennis en informatie over de school als het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen en de naam van de school niet schaadt.*
   Privé-meningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de school en/of het bestuur.

   Je blijft altijd persoonlijk verantwoordelijk voor wat je deelt of publiceert. Wees je ervan bewust dat gepubliceerde uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na het verwijderen van het bericht.

5. *Ga voordat je foto's of video's publiceert, waar leerlingen herkenbaar op te zien zijn, na of ouders hiervoor toestemming hebben gegeven.*
   Meer informatie hierover is te vinden in het onderdeel 'Toestemming foto's, video's en online diensten'.

6. *Gebruik de accounts die door Fluvium worden beheerd als je met anderen wil communiceren via e-mail of social media.*
   Formuleer je boodschap ook hier professioneel en zorgvuldig. Het is uiteraard ook goed om vanuit ParnasSys te mailen.

7. *Zet e-mailadressen altijd in de BCC-regel als je naar (grote) groepen mensen een bericht verstuurt.*
   Zo blijven de e-mailadressen van de groepsleden afgeschermd.

8. *Overweeg een bericht met belangrijke of gevoelige informatie na te laten lezen door een collega voordat je het verstuurt naar (een groep) ouders/verzorgers.*
   Een foutje is snel gemaakt en bovendien kan een ander je boodschap anders interpreteren dan jij hem bedoeld hebt. Het is dan fijn als er iemand met je meeleest voordat je hem verstuurt.

9. *Vragen of klachten over privacy worden in eerste instantie beantwoord door de directeur. De directeur kan de vraag eventueel doorzetten aan de Privacy Officer.*

C. Hoe houd ik indringers op afstand?

1. *Zorg er bij vertrouwelijke (telefonische) gesprekken voor dat er niet kan worden meegeluisterd.*
   Trek je je even terug als een gesprek een vertrouwelijk karakter heeft of krijgt.

2. *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 te komen. Ook kunnen de gegevens op je computer versleuteld worden (ransomeware).

3. *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 bij de printer.*
   Met de combinatie van de Windows- en L-toets of voor een Chromebook Zoeken + L of met het 'Slot teken', kun je je makkelijk afmelden. 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.

4. *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.

5. *Laat je wachtwoorden van ParnasSys en Raet 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 kan dan dus ook inloggen. Maak gebruik van wachtwoordkluisjes, zoals Last Pass of True Key. Kijk **hier** voor een tip om een sterk wachtwoord te kiezen die je makkelijk kunt onthouden.

6. *Houd je logingegevens altijd voor jezelf, ook al vragen anderen aan je om ze te delen.*
   Je login is in feite een sleutel om toegang te krijgen tot de informatie die voor jou toegankelijk moet zijn. Daarnaast herkent het systeem jou door je login, zodat het kan bijhouden wie welke gegevens heeft bekeken, toegevoegd of gewijzigd.

In het verlengde van bovenstaande is het ook van belang dat leerlingen zich bewust zijn van risico's en er goede afspraken met hen gemaakt worden in het kader van privacy. In **bijlage H** is een voorbeeld opgenomen van dergelijke afspraken. Dit model is naar eigen inzicht aan te passen aan de visie en werkwijze van de school. Van iedere school wordt verwacht dat ze een dergelijk protocol hebben en toepassen.

Privacyreglement

Volgens de nieuwe wet ben je als school(bestuur) verplicht om nieuwe en bestaande ouders van leerlingen, duidelijk te informeren over wat de school met de persoonsgegevens van hun en hun kinderen doet. Ook medewerkers dienen duidelijk geïnformeerd te worden over wat er met hun gegevens gebeurt.
Met het privacyreglement voldoet Fluvium aan deze informatieplicht. In het reglement wordt duidelijk gemaakt (transparant) 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).

Ook is hierin te lezen hoe de toegang is geregeld, hoe de gegevens zijn beveiligd en met wie ze uitgewisseld mogen worden.
Het reglement is in te zien via de website www.stichtingfluvium.nl. Het reglement is ook als **bijlage A** toegevoegd bij dit handboek.

Ouders worden via het inschrijfformulier en via de website van de scholen gewezen op het privacyreglement.

Toestemming

Beeldmateriaal van leerlingen
Ouders moeten altijd toestemming geven voor het gebruik van beeldmateriaal van hun kinderen. Die toestemming moet specifiek zijn. Dat betekent dat het voor ouders duidelijk moet zijn voor welk gebruik van het beeldmateriaal ze toestemming geven. Bijvoorbeeld voor het gebruik op de website, in een nieuwsbrief of de schoolgids. Hiervoor vullen ouders bij inschrijving een toestemmingsformulier gebruik beeldmateriaal in, zie **bijlage D**.
Ouders moeten ook de mogelijkheid hebben deze toestemming te wijzigen. Zij worden jaarlijks actief aan deze mogelijkheid herinnerd middels een bericht in de eerste nieuwsbrief van het jaar.
Gegeven toestemming wordt geregistreerd in ParnasSys. Wanneer een medewerker van Fluvium beeldmateriaal van een leerling wil gebruiken, dient daarvoor eerst ParnasSys geraadpleegd te worden. Dit kan ook via de groepsleerkracht.

Beeldmateriaal van medewerkers
Voor gebruik van beeldmateriaal van medewerkers moet in principe ook toestemming gevraagd worden. Deze toestemming dient ook vastgelegd te worden. Wanneer het beeldmateriaal alleen voor intern gebruik is, dan is deze toestemming geregeld middels een bijlage bij de aanstelling. Een medewerker mag op elk moment bezwaar maken tegen het gebruik van zijn/haar beeldmateriaal. Dit kan via privacy@stichtingfluvium.nl en/of via de schoolleiding van de eigen school.

Beeldopnames door ouders
Soms zijn er in de school ook ouders die foto's of video's maken bijvoorbeeld bij feestelijke gelegenheden, zoals het afscheid van groep 8 of een verjaardag maar ook bijvoorbeeld bij de eerste schooldag of een sportdag of het bezoek van Sinterklaas. Het maken van beeldmateriaal, mits niet storend is toegestaan voor privé-gebruik. Het is niet toegestaan om foto- of video-opnames die gemaakt zijn op school te delen via sociale media of te gebruiken voor commerciële doeleinden. Je kunt dit kenbaar maken door deze afspraak op te nemen in de schoolgids en/of op de website.

Beeldopnames voor begeleidingsdoeleinden
Op de scholen binnen Fluvium zijn regelmatig studenten aanwezig om stage te lopen. Deze studenten worden begeleid door een coach vanuit de PABO. Deze coach wil soms voor trainingsdoeleinden beeldopnames maken van de studenten en/of hun mentor terwijl zij bezig zijn met lesgevende taken. De PABO gebruikt dit materiaal alleen als bewijs dat de student iets heeft bereikt/gedaan, daarna worden de beelden vernietigd. Studenten mogen deze beelden ook niet voor andere doeleinden gebruiken. In dergelijke situaties is de PABO (en niet Fluvium) verantwoordelijk voor de privacy van de personen die herkenbaar in beeld komen.

Als de scholen binnen Fluvium hun eigen leerkrachten willen coachen/trainen aan de hand van beeldopnames, is Fluvium wél verantwoordelijk.

Om in dat geval voor trainingsdoeleinden tijdens de les te kunnen filmen, moet je aan de volgende voorwaarden voldoen:

Voorwaarden

1. Leg de docent in kwestie uit waarom je hem wilt filmen en vraag vervolgens schriftelijk of per mail om toestemming;
2. Film vanuit achterin het lokaal, zodat de leerlingen alleen 'op de rug' worden gefilmd. Zo breng je de kinderen niet herkenbaar in beeld en zijn ze niet meer identificeerbaar. Dit heeft als grote voordeel dat je volgens de AVG voor wat betreft de kinderen geen persoonsgegevens meer aan het verwerken bent. Wil je de kinderen wél identificeerbaar in beeld brengen? Dan val je weer onder de AVG en is voorafgaande toestemming van de ouders nodig.
3. Zet de beelden op een GoogleDrive en wis het filmpje op de camera;
4. Laat het filmpje niet aan derden zien, die niet betrokken zijn bij het proces en verstrek het ook niet aan derden;
5. Spreek met de docent af dat hij dit ook niet mag doen;
6. Verwijder het filmpje aan het einde van de coaching.

Binnen Fluvium wordt gebruik gemaakt van Iris Connect. Dit is een applicatie waarmee video-opnames voor coaching doeleinden veilig bewaard en gedeeld kunnen worden. Met Iris Connect is een verwerkersovereenkomst afgesloten.

Uitwisseling persoonsgegevens

Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een arbo- of schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Deze toestemming hoeft niet ieder jaar opnieuw gevraagd te worden maar wel als er een nieuw traject wordt gestart, andere hulpverleners betrokken worden of de omstandigheden om andere redenen veranderen. Zorg dat je de toestemming registreert en houd daarbij ook rekening met de verdeling van het ouderlijk gezag. Voor de uitwisseling van leerlinggegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. In het volgende hoofdstuk lees je hierover meer. Neem bij twijfel contact op met je directeur of IB-er.

Wanneer je persoonsgegevens van leerlingen en/of hun ouders uit wil wisselen met andere ouders, bijvoorbeeld als je klassenlijsten wil verspreiden, heb je altijd toestemming van ouders nodig. Ouders kunnen op het inschrijfformulier aangeven of zij hier toestemming voor geven.

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.

Toestemming voor het gebruik van online diensten kunnen ouders ook aangeven op het toestemmingsformulier bij inschrijving. Een andere mogelijkheid is om de ouders te verzoeken het account zelf thuis voor het kind aan te maken. In dat geval hoeft de school geen toestemming te vragen.

Eisen mobiele devices

De mobiele devices in eigendom van de medewerker kunnen gebruikt worden voor schoolwerkzaamheden indien ze voorzien zijn van de volgende beveiligingseisen, zodat persoonsgegevens goed beschermd zijn.

- Het device is voorzien van een wachtwoord of code.
- Het device is voorzien van up-to-date softwarebeveiliging.
- E-mail en andere apps of online toepassingen van Fluvium moeten afgeschermd worden met een apart wachtwoord. *Vind je het lastig om meerdere werkgerelateerde wachtwoorden te onthouden? Gebruik dan een wachtwoordkluisje van Last Pass, KeePass of True key. Daarmee kun je zakelijk en privé op een veilige manier scheiden op je eigen device. En hoef je maar 1 wachtwoord te onthouden.*
- E-mail en andere apps of online toepassingen mogen niet toegankelijk zijn voor andere gebruikers.
- Er worden geen bestanden lokaal opgeslagen, maar alleen op de daarvoor aangewezen bewaarplaatsen van Fluvium.
- Er worden geen leerlinggegevens op devices verwerkt die gebruikt worden in openbare netwerken. Dit zijn netwerken waar je zonder wachtwoord in te geven verbinding met internet mee kunt maken. Werk alleen op betrouwbare netwerken.

Uitwisseling persoonsgegevens

Wanneer je gegevens van leerlingen uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het meestal nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en houd daarbij ook rekening met de verdeling van het ouderlijk gezag.

Voor de uitwisseling van leerlinggegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Kijk hieronder in de tabel met welke partijen je gegevens mag uitwisselen en op welke manier.

Wanneer je gegevens van medewerkers uitwisselt met externen, zoals het administratiekantoor, DUO of de arbo-arts dan is dit in de meeste gevallen geregeld in de wet of de arbeidsovereenkomst. Wanneer dat niet het geval is zal je ook hiervoor toestemming moeten vragen van de betreffende medewerker. Meer hierover vind je in deel B.

Verstrekking aan	Doel	Uitwisseling toegestaan	Wijze waarop	Toestemming nodig?
Dienst Uitvoering Onderwijs	Bekostiging*	Ja	Koppeling ParnasSys	Nee
Educatieve uitgeverijen en Basispoort	Gebruik digitale leermiddelen	Ja	Koppeling ParnasSys	Nee
Basisscholen of scholen voor voortgezet onderwijs	Overdracht leerlingdossier (na aanmelding)*	Ja	Koppeling OSO	Nee (wel inzage)
Externe Onderwijs-specialisten	Zorgbegeleiding van een leerling	Ja	Verstrekken account	Ja
Stagiaires	Opleiden	Ja	n.v.t.	Nee, wel overeenkomst
Samenwerkings-verband	Toelaatbaarheids-verklaring afgeven*	Ja, zie ook: https://passendonderwijsenprivacy.nl	n.t.b. nu nog via de mail	Nee
schoolbieb	Leesmonitor	Ja	n.t.b.	Ja

Verstrekking aan	Doel	Uitwisseling toegestaan	Wijze waarop	Toestemming nodig?
GGD/JGZ	Bezoek schoolarts	Nee	n.v.t. haalt info uit BRON	n.v.t.
Inspectie van het onderwijs	Toezicht*	Ja	Via ISD (internet schooldossier)	Nee
Leerplicht Gemeente	Controle verzuim	Ja	Verzuimloket	Nee

* Wettelijk verplicht

Gemeente en leerplichtambtenaren
De gemeente vraagt soms om informatie van leerlingen voor gemeentebeleid. Ook belt soms de leerplichtambtenaar voor een specifiek geval. Hoewel dit officiële instanties zijn, hebben zij niet altijd recht op informatie. De leerplichtambtenaar heeft bijvoorbeeld geen recht op (wettelijke grondslag voor) andere gegevens dan die behoren tot het onderwijskundig rapport (OKR) en kan deze dus alleen met toestemming van de ouders krijgen. 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 andere organisaties. Gegevens kun je veilig uitwisselen door ze te delen in plaats van te mailen, dat wil zeggen de gegevens worden opgeslagen in Google Drive, in een map en dan deel je het document of de map met de betreffende persoon of instanatie. Hierdoor hoeven er geen persoonsgegevens gemaild te worden en behoud je zelf de regie over met wie en voor hoe lang je de gegevens deelt.

Samenwerkingsverbanden
Voor de uitwisseling van leerlinggegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Hiervoor kun je terecht bij de Intern Begeleider. Kijk op **https://passendonderwijsenprivacy.nl** voor meer informatie over privacy en samenwerkingsverbanden.

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 haar toezichttaken vraagt de inspectie om documenten aan te leveren. Deze gegevens dienen zoveel 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. Neem bij twijfel contact op met de directeur.

Burger Service Nummer (BSN)
Ons Nederlands recht schrijft voor dat je het BSN alleen mag verwerken als dit in de wet is bepaald óf als de doeleinden waarvoor je het verwerkt bij wet zijn bepaald.[1] Voor scholen betekent dit het volgende.

Een school mag/moet het BSN van een leerling verwerken:
1. Bij de toelating van een leerling tot de school;[2]
2. Door het nummer in de leerlingenadministratie van de school op te nemen;[3]
3. In het contact met de leerling (of zijn ouders);
4. Door het BSN aan de minister van OCW te verschaffen;
5. In het contact met deze minister over de bekostiging van de school;
6. In het contact met een gemeente in het kader van de Leerplichtwet;
7. In het contact met een andere school t.b.v. in- of uitschrijven en overleggen OKR;
8. Ter uitvoering van subsidieregelingen van het Europees Sociaal Fonds
9. In contacten met een andere school die valt onder de Wet op Expertise Centra t.b.v. de ondersteuning die deze school biedt;
10. Als eenmalige verwerking bij het aanmaken van een pseudoniem voor een leerling met het oog op het aanbieden van onderwijsvoorzieningen en begeleiding aan deze leerling;
11. Om het pseudoniem te bewaren in een leerlingregistratiesysteem.

Een school mag het BSN van een leerling dus alleen in deze gevallen of voor deze doeleinden verwerken.

[1] Art. 46 Uitvoeringswet AVG
[2] Art. 40 b Wet op het primair onderwijs
[3] Voor punt 2 t/m 11 is de grondslag: art. 178a Wet op het primair onderwijs

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 via je schooldirecteur of via **privacy@stichtingfluvium.nl** in verband met de meldplicht 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 de volgende incidenten:

- een e-mail die aan een verkeerd persoon is geadresseerd
- een kwijtgeraakte USB-stick*
- inloggegevens die openbaar zijn geworden
- een gestolen device*
- een gehackte device*

*waarop persoonsgegevens staan

Het College van Bestuur van de school is verantwoordelijk 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 bij je schooldirecteur en/of via **privacy@stichtingfluvium.nl**.

Je wordt dan gevraagd om een formulier in te vullen met een aantal gegevens over het beveiligingsincident (zoals datum, tijd, aard van de gegevens etc.). Op basis van deze informatie kan beoordeeld worden of er sprake is van een datalek en of het nodig is om verdere maatregelen te treffen.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

In **E. Procedure datalekken** is de volledige procedure melden datalekken opgenomen.

Toegangsbeleid

Binnen Fluvium zijn de leden van een schoolteam gezamenlijk verantwoordelijk voor de zorg voor hun leerlingen. Zij dragen daarom ook gezamenlijke verantwoordelijkheid voor het zorgvuldig omgaan met de privacy van zowel de teamleden, de leerlingen en hun ouders.

Fluvium vertrouwt op de integriteit en het privacybewustzijn van haar medewerkers. Binnen Fluvium weet het personeel dat je niet zomaar in de persoonsgegevens van leerlingen mag kijken waar jij in je werk niet mee te maken hebt, of in de persoonsgegevens van je collega's. Van medewerkers wordt verwacht dat zij kunnen uitleggen waarom zij bepaalde persoonsgegevens hebben ingezien voor de uitoefening van hun werk.

Om eventueel oneigenlijk gebruik te voorkomen en op te sporen voert Fluvium controles uit. Dit betekent dat periodiek en steekproefsgewijs aan de hand van logging wordt bekeken door welke medewerkers persoonsgegevens zijn geraadpleegd of gewijzigd. Zo nodig, wordt op deze logging gehandeld en worden medewerkers aangesproken op hun gebruik van de systemen. Leidend is ook hier dat Fluvium van haar medewerkers verwacht dat zij kunnen uitleggen waarom zij bepaalde persoonsgegevens hebben ingezien.

Deze logging taak ligt bij de, directeur en zal minimaal tweemaal per schooljaar worden uitgevoerd. De Privacy Officer ziet er op toe dat de controle gebeurt, door de directeuren actief te bevragen en zijn bevindingen vast te leggen in een logboek.

Voor stagiairs en tijdelijke medewerkers/zzp'ers is de toegang tot de systemen beperkt. Zij krijgen alleen toegang tot de persoonsgegevens van de eigen klas/leerling waarmee zij te maken hebben. De directeur is verantwoordelijk voor het verstrekken van deze accounts en ziet er op toe dat de deze accounts weer worden ingetrokken na afloop van de stage/werkzaamheden.

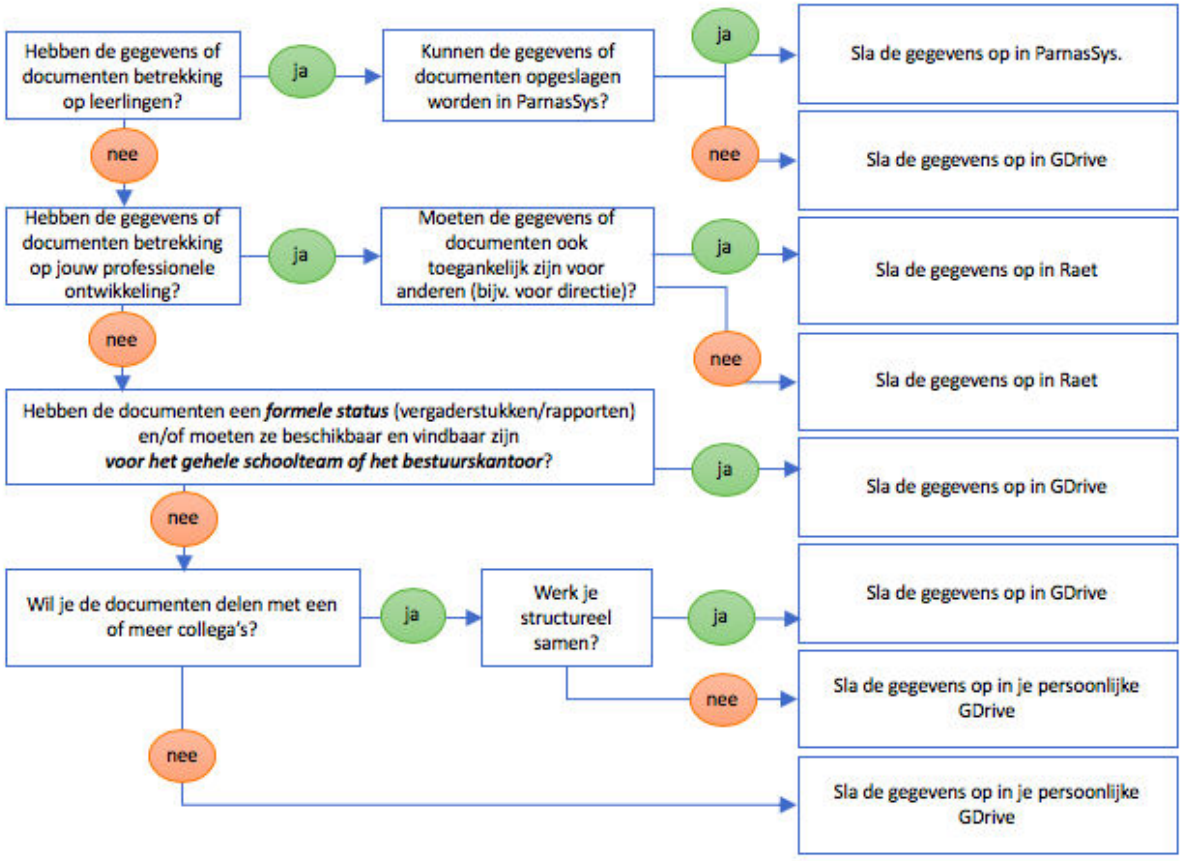
Naast het toepassen van dit toegangsbeleid worden de volgende beveiligingsmaatregelen toegepast op systemen waarin persoonsgegevens worden gebruikt:

- Inloggegevens worden verstuurd naar het e-mailadres van de medewerker dat beheerd wordt door (een school van) het bestuur.
- Inloggegevens worden periodiek (minstens 1x per jaar) vernieuwd.
- Er wordt technisch afgedwongen (waar mogelijk) om sterke wachtwoorden te gebruiken.

Document- en datamanagement

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 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 op moet slaan.



Levende documenten
Wanneer gegevens gedurende een proces verwerkt worden in een 'levend' document kan er voor gekozen worden om zo'n document gedurende het proces op te slaan in de GDrive. Wanneer er structureel samengewerkt wordt kan dit een gedeelde map zijn, zoals bijvoorbeeld in het geval van groeidocumenten voor zorgleerlingen. Groeidocumenten worden gedurende het proces opgeslagen in de daarvoor aangemaakte map in de GDrive. Deze map wordt beheerd door de interne begeleider. Wanneer het groeidocument compleet is wordt het opgeslagen in ParnasSys en verwijderd uit de GDrive.
Voor documenten die betrekking hebben op de professionele ontwikkeling van medewerkers

geldt een soortgelijk proces. Deze documenten kunnen gedurende het proces gedeeld worden vanuit de daarvoor aangemaakte map op de GDrive. Wanneer de documenten compleet zijn worden ze opgeslagen in Raet en verwijderd uit de GDrive.

LAS
Op verschillende scholen wordt naast ParnasSys ook gebruik gemaakt van andere systemen. Medewerkers houden zich hierbij aan de gedragscode. In het register voor de gegevensverwerkingen is te lezen wat voor soort gegevens hierin worden opgeslagen en hoe de toegang is geregeld.

Inschrijfformulieren en Parro-app
Voor inschrijfformulieren geldt dat deze worden ingescand en opgeslagen in ParnasSys. Dit is belangrijk omdat de school een kopie met handtekening moet bewaren. Scholen die gebruik maken van de Parro-app, kunnen hierin toestemming regelen.

Klassenmap
In elke klas is een klassenmap aanwezig met daarin praktische informatie voor de organisatie van het onderwijs in de betreffende groep. Deze klassenmap ligt doorgaans op het bureau van de leerkracht. Hoewel de algemeen aanvaarde norm binnen Fluvium is dat niemand ongevraagd aan de spullen van een ander komt, kan niet uitgesloten worden dat de informatie in de klassenmap terecht komt bij onbevoegden. Het is daarom van belang dat er in de klassenmap alleen persoonsgegevens staan vermeld die voor de leerkracht noodzakelijk zijn om frequent en acuut in de klas voorhanden te hebben. Persoonsgegevens die daar niet onder vallen, worden opgeslagen in het digitale dossier.

Bewaar nooit wachtwoorden in de klassenmap!
Informatie die noodzakelijk is voor een invaller zal per groep bij de directeur/IB-er (of een ander aanspreekpunt voor de invaller) aanwezig zijn en bij aanvang van het invallen met de betreffende leerkracht gedeeld worden. Denk hierbij aan de benodigde wachtwoorden, noodzakelijke medische gegevens (bv. EpiPen of voedselallergie) of belangrijke informatie over de thuissituatie.

Deel B

Informatie voor directeur en leidinggevenden

Deel B geeft antwoord op de volgende vragen

- Wat moet ik met **ouders** regelen rondom privacy?
- Welke **afspraken** moet ik maken met mijn medewerkers in het kader van privacy?
- Wat moet ik weten over **datalekken**?
- Wat moet ik weten als het gaat om het **verlenen van toegang** tot persoonsgegevens?
- Hoe lang moet ik persoonsgegevens **bewaren**?
- Welke afspraken maak ik over devices die in **bruikleen** worden gegevens?
- Wat moet ik weten over **externe partijen** die namens de school persoonsgegevens verwerken?
- Welke **rollen en verantwoordelijkheden** t.a.v. IBP zijn er binnen de schoolorganisatie belegd?
- Hoe kan ik aantonen dat ik IBP **op orde** heb?

Ouders en privacy

Privacyreglement
Ouders hebben het recht om te weten welke gegevens er van hen en van hun kinderen worden verzameld door de school en voor welke doeleinden deze gegevens verzameld worden. Met het privacyreglement voldoet het bestuur aan zijn wettelijke informatieplicht, mits deze ook actief wordt aangeboden aan de ouders[4]. Daarom is het voor scholen belangrijk om het privacyreglement met ouders te communiceren.

In **bijlage B** is een tekst opgenomen die door alle scholen binnen het bestuur gebruikt wordt om ouders via de website en de schoolgids te wijzen op het privacyreglement van de school. Het kan in sommige gevallen nodig zijn om deze tekst uit te breiden indien er op school aanvullende bijzondere persoonsgegevens verwerkt worden. Ouders kunnen het reglement ook opvragen bij de directie van de school.

Toestemming
Voor het gebruik van foto- en filmopnames van leerlingen en medewerkers is toestemming vereist. Het handigste is om de toestemming voor het gebruik van foto-en filmopnames direct bij de inschrijving van een leerling of indiensttreding van een werknemer te regelen.
Om dit via voor leerlingen te regelen is binnen ons bestuur een tekst voor het toestemmingsformulier beschikbaar gesteld. De tekst is te vinden in **bijlage D.** Hierop geven ouders aan of zij toestemming geven voor het gebruik van beeldmateriaal en voor welke doeleinden.
Als directeur is het belangrijk om ouders jaarlijks te herinneren (bijvoorbeeld via de nieuwsbrief en in de schoolgids) dat deze toestemming herroepen of alsnog verleend kan worden.
Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een arbo- of schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en hou daarbij ook rekening met de verdeling van het ouderlijk gezag.

Gezagsregister
Elk minderjarig kind staat onder gezag. Gezag van zijn ouders (ouderlijk gezag) of van een verzorger/voogd (voogdij). Aan ouders die getrouwd zijn of een geregistreerd partnerschap hebben, komt het ouderlijk gezag *gezamenlijk* toe. Dit volgt uit de wet. Als de ouders vervolgens scheiden, verandert er in principe niets aan het ouderlijk gezag: dat komt nog steeds beide ouders gezamenlijk toe. Op deze standaard gezinssituaties zijn veel uitzonderingen mogelijk. Dan komt het gezag slechts aan één van de ouders toe of aan een voogd. In het gezagsregister van de rechtbank wordt per minderjarig kind bijgehouden wie het gezag heeft. De school doet er goed aan om het gezagsregister te raadplegen om op de hoogte zijn van de actuele verdeling van het gezag over zijn leerlingen.

[4] Ouders kan desgewenst ook gelezen worden als verzorgers.

Gezamenlijk ouderlijk gezag is niet twee keer toestemming vragen
Als aan beide ouders het ouderlijk gezag gezamenlijk toekomt, hoeft de school niet aan beide ouders om toestemming te vragen. Het is verdedigbaar dat de school afgaat op de (weigering van) toestemming van één van de ouders. Hiervoor zijn twee redenen:

1. De letterlijke tekst van de AVG spreekt in enkelvoud: de persoon die de ouderlijke verantwoordelijkheid draagt. Dit veronderstelt dat - indien de ouderlijke verantwoordelijkheid bij beide ouders ligt - toestemming van één daarvan voldoende is voor rechtsgeldigheid.

2. Er is een parallel te trekken met de regeling in het Burgerlijk Wetboek voor zorgbehandelingen aan kinderen. Daar staat dat je er als zorgaanbieder in principe van uit mag gaan dat de toestemming van één ouder mede namens de andere ouder geldt, tenzij er aanwijzingen zijn dat de afwezige ouder bezwaar heeft bij het aanbieden van zorgbehandelingen. Ouders moeten zelf kenbaar maken als ze er onderling samen niet uitkomen.

Als later blijkt dat de andere ouder het niet eens is met de toestemming van de ene ouder, ontneemt dat de rechtsgeldigheid van de toestemming niet. Vanaf het moment dat de andere ouder protesteert, moet je de verwerking wel stopzetten totdat beide ouders weer op één lijn zitten. Bij verschil van mening gaat nee altijd boven ja.

Voorlichting en bewustwording onder medewerkers

Om informatiebeveiliging en privacy goed op orde te hebben is het nemen van maatregelen en het inrichten van procedures alleen niet voldoende. Het is minstens zo belangrijk dat iedereen binnen de organisatie op de hoogte is van deze maatregelen en procedures en dat er goede afspraken gemaakt worden met de medewerkers. Deze afspraken staan beschreven in het volgende hoofdstuk.

In dit hoofdstuk lees je wat er binnen Fluvium gedaan wordt en wat er van jou als schooldirecteur gevraagd wordt om medewerkers bewust te maken van het belang van informatiebeveiliging en privacy.

Medewerkers zullen de uitgangspunten van de AVG in hoofdlijnen moeten begrijpen om zelf de juiste afweging te maken als het gaat om het verwerken van persoonsgegevens. En zij zullen daarbij actief op de hoogte gehouden moeten worden van nieuwe ontwikkelingen rondom de privacywetgeving. Bij nieuwe processen binnen de organisatie is het belangrijk om daarbij ook te kijken naar de impact op het IBP-beleid. Je kan hierbij denken aan het in gebruik nemen van een communicatie-applicatie, het aanschaffen van nieuwe (digitale) leermiddelen of het invoeren van groepsdoorbrekend werken. Is er sprake van nieuwe risico's, moeten er aanvullende maatregelen genomen worden of afspraken gemaakt worden?

Bovenschools
Tijdens voorlichtingssessies, bij de implementatie van dit handboek in 2018, met de teams is er uitgebreid stilgestaan bij de wetgeving en het IBP-beleid van Fluvium.
Naast deze voorlichtingsmiddagen worden de scholen voorzien van voorlichtingsmateriaal voor zowel medewerkers als leerlingen en hun ouders.

Wanneer er nieuwe ontwikkelingen zijn met betrekking tot de AVG en het IBP-beleid van Fluvium zal de privacy officer dit in overleg met de functionaris gegevensbescherming en het College van Bestuur (CvB) communiceren met de directeuren. Daarnaast zal er jaarlijks, in de eerste maanden van het schooljaar, onder leiding van de privacy officer, bovenschools een risicoanalyse uitgevoerd worden samen met de directeuren. De situatie op de scholen wordt hierin meegenomen. Waar mogelijk worden hieruit voortvloeiende maatregelen, procedures en afspraken bovenschools geregeld.

Tijdens bovenschoolse IB- en ICT-bijeenkomsten zal het onderwerp IBP ook regelmatig aan de orde komen. Bijvoorbeeld wanneer er nieuwe verwerkingen of technologieën ingevoerd worden of wanneer er aanleiding is om maatregelen te bespreken die voortkomen uit de risicoanalyses.

Schooldirecteuren
De school is een veilige werkplek waar met respect en aandacht voor ieders privacy gehandeld wordt. Als schooldirecteur heb je de taak om hierover zowel formeel als informeel het gesprek te voeren met je medewerkers.

Van directeuren wordt verwacht dat zij regelmatig stil staan bij het IBP-beleid op hun school, bijvoorbeeld tijdens een studiedag of teamvergadering. Er kan dan met het team gekeken worden naar mogelijke risico's en benodigde maatregelen. IBP-beleid op schoolniveau dient tevens opgenomen te zijn in het schoolplan. Hierin is duidelijk aangegeven welke acties er op school ondernomen worden m.b.t. IBP en wie daarvoor verantwoordelijk is binnen het team.

Wanneer medewerkers nieuw zijn op school wordt in de inwerkperiode expliciet aandacht besteed aan de afspraken die er binnen Fluvium zijn rondom de verwerking van persoonsgegevens en het belang van informatiebeveiliging.
Het zal ook onderwerp van gesprek zijn in de informatiebijeenkomst voor nieuwe medewerkers. De informatie is tevens beschikbaar via het intranet.

Afspraken met medewerkers

In deel A van dit handboek zijn gedragsregels rondom informatiebeveiliging en privacy opgenomen die voor alle medewerkers binnen het bestuur gelden. Deze zijn hieronder in het kort weergegeven.

Het is belangrijk om medewerkers bewust te maken van het belang van deze regels rondom IBP en de gedragscode in te bedden in de schoolcultuur.

Laat de gedragsregels regelmatig terugkomen in gesprekken en tijdens overleggen. Besteed expliciet aandacht aan het hanteren van de Vuistregels Privacy bij het verzamelen en uitwisselen van gegevens.

A. Waar en hoe bewaar ik persoonsgegevens?

1. Verwerk persoonsgegevens digitaal in de daarvoor aangewezen bewaarplaatsen.
2. Formuleer gegevens die je vastlegt over een persoon zorgvuldig en professioneel.
3. Wanneer je persoonsgegevens verwerkt maak je altijd gebruik van de beveiligde Google Drive omgeving. Je slaat dus nooit gegevens op op je eigen computer of device.
4. Ga na welke afspraken er binnen de school gemaakt zijn voordat je persoonsgegevens uitwisselt met derden.
5. Informeer derden (ouders, hulpverleners etc.) wanneer je door hen aangeleverde informatie (zowel geschreven als mondeling) opslaat in het leerlingdossier.

B. Hoe en wat communiceer ik online?

1. Maak gebruik van een link naar het digitaal administratiesysteem om persoonsgegevens uit te wisselen met collega's.
2. Vraag ouders om toestemming om een (privé)account aan te maken voor online diensten.
3. Deel over leerlingen, ouders of collega's nooit informatie via social media.
4. Deel alleen kennis en informatie over de school als het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen en de naam van de school niet schaadt.
5. Ga voordat je foto's of video's publiceert waar leerlingen op te zien zijn na of ouders hiervoor toestemming hebben gegeven, zoals in ParnasSys weergegeven.
6. Gebruik de accounts die door de school worden beheerd als je met anderen wil communiceren via e-mail of social media.
7. Zet e-mailadressen altijd in de BCC-regel als je naar (grote) groepen mensen een bericht verstuurt.
8. Wanneer je een bericht stuurt met belangrijke en/of gevoelige informatie naar (een groep) ouders/verzorgers laat dit dan bij voorkeur nalezen door een collega.

C. Hoe houd ik indringers op afstand?

1. Zorg er bij vertrouwelijke (telefonische) gesprekken voor dat er niet kan worden meegeluisterd.

2. Bewaar laptops of tablets altijd op een veilige plek, zeker tijdens vakantieperiodes.
3. Klik alleen op linkjes en open alleen bijlagen in e-mails van betrouwbare afzenders en pas op met het downloaden van bestanden.
4. 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 bij de printer.
5. 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.
6. Houd je logingegevens altijd voor jezelf, ook al vragen anderen aan je om ze te delen.

Uitwisseling persoonsgegevens

Wanneer je gegevens van medewerkers uitwisselt met externen, zoals het administratie-kantoor, DUO of de Arboarts, dan is dit in de meeste gevallen geregeld in de wet of de arbeidsovereenkomst. Wanneer dat niet het geval is zal je hiervoor toestemming moeten vragen van de betreffende medewerker.
Kijk hieronder in de tabel met welke partijen je gegevens mag uitwisselen en op welke manier.

Verstrekking aan	Doel	Uitwisseling toegestaan	Wijze waarop	Toestemming nodig?
Dienst Uitvoering Onderwijs	Bekostiging*	Ja	Koppeling ParnasSys	Nee
Educatieve uitgeverijen en Basispoort	Gebruik digitale leermiddelen	Ja	Koppeling ParnasSys	Nee
Basisscholen of scholen voor voortgezet onderwijs	Overdracht leerlingdossier (na aanmelding)*	Ja	Koppeling OSO	Nee (wel inzage)
Externe Onderwijs-specialisten	Zorgbegeleiding van een leerling	Ja	Verstrekken account	Ja
Administratie-kantoor	Salarisadministratie en HR-management (werkt in Raet)	Ja	n.t.b.	Nee
UWV			Raet/mail	
Vervangingsfonds	Subsidieaanvraag	Ja	Post/mail	Ja
IPPON	Vervanging	Ja	DOTO	Nee
Participatiefonds	Instroomtoets (vergoeding ww)	Ja	Beveiligde omgeving	Nee
Robidus	Administratie langdurig ziekteverzuim	Ja	Beveiligd platform HR-controlnet	Nee
Loyalis	Premievastestelling verzekering	Ja	Beveiligde link?	Nee (behalve bij subisidie aanvraag)

* Wettelijk verplicht

Protocol melden datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete. De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in de leerlingadministratie of digitale leermiddelen.

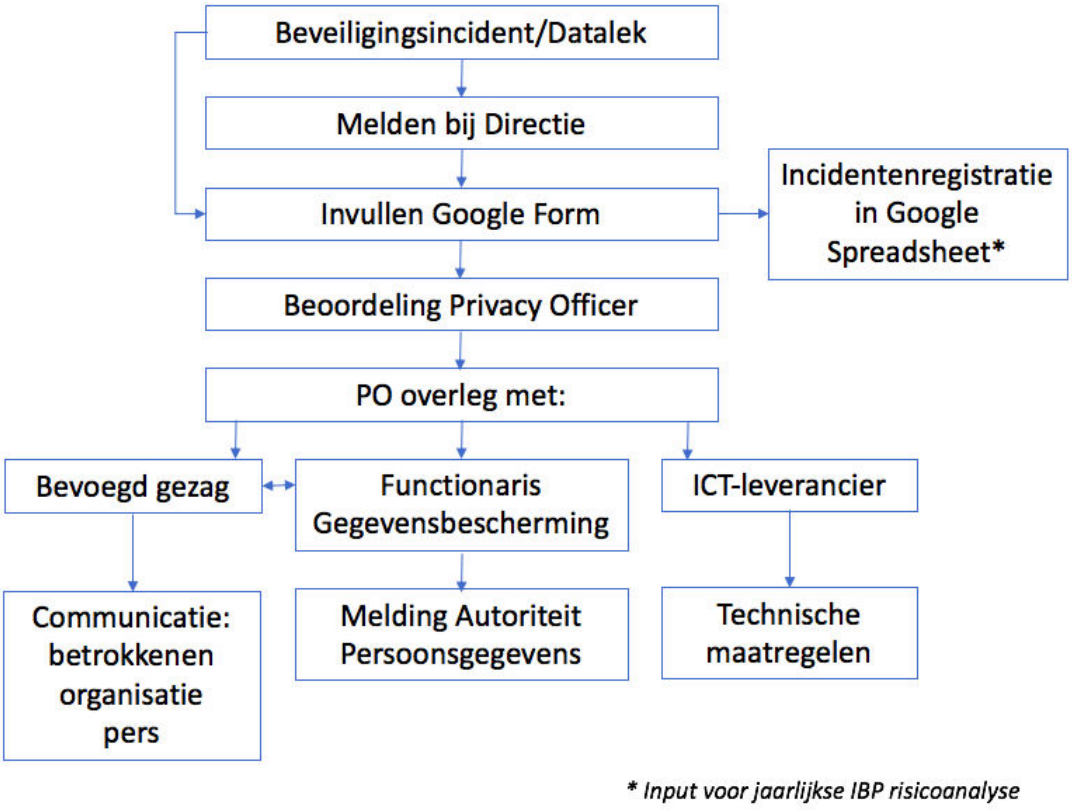
Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten dat persoonsgegevens verloren zijn gegaan. Wanneer derden toegang hebben gekregen tot persoonsgegevens, die geen toegang hadden mogen hebben of wanneer gegevens (tijdelijk) niet meer beschikbaar zijn is er ook sprake van een datalek.
Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van klas 3b, is ook een datalek.

Wanneer een van je medewerkers een beveiligingsincident of datalek ontdekt kan diegene dit direct melden via **privacy@stichtingfluvium.nl**. Er dient dan een formulier ingevuld te worden met vragen over het incident. Het is ook mogelijk om dit via de directeur te doen. In dat geval vullen jullie samen het meldingsformulier is.

De melding wordt geregistreerd door de privacy officer. De privacy officer maakt een eerste inschatting van het incident en gaat indien nodig in overleg met het bevoegd gezag, de functionaris van de gegevensbescherming (FG) en/of de ICT-leverancier. Wanneer het een ernstig datalek betreft zal de FG een melding doen bij de Autoriteit Persoonsgegevens. Indien nodig zal het bevoegd gezag betrokkenen informeren en eventueel ook de (rest van de) organisatie en in een enkel geval zelfs de pers.

De privacy officer houdt een register bij van alle meldingen en vervolgacties. Het register datalekken wordt binnen Fluvium gebruikt om risico’s te analyseren en benodigde maatregelen te bepalen.

Hieronder is schematisch weergegeven hoe de procedure datalekken er binnen Fluvium uitziet.



Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

De volledige procedure datalekken is te vinden in **bijlage E**.

Toegangsbeleid

Binnen Fluvium zijn de leden van een schoolteam gezamenlijk verantwoordelijk voor de zorg voor hun leerlingen. Zij dragen daarom ook gezamenlijke verantwoordelijkheid voor het zorgvuldig omgaan met de privacy van zowel de teamleden, de leerlingen en hun ouders.

Fluvium vertrouwt op de integriteit en het privacybewustzijn van haar medewerkers. Binnen Fluvium weet het personeel dat je niet zomaar in de persoonsgegevens van leerlingen mag kijken waar jij in je werk niet mee te maken hebt, of in de persoonsgegevens van je collega's. Van medewerkers wordt verwacht dat zij kunnen uitleggen waarom zij bepaalde persoonsgegevens hebben ingezien voor de uitoefening van hun werk.

Om eventueel oneigenlijk gebruik te voorkomen en op te sporen voert Fluvium controles uit. Dit betekent dat periodiek en steekproefsgewijs aan de hand van logging wordt bekeken door welke medewerkers persoonsgegevens zijn geraadpleegd of gewijzigd. Zo nodig, wordt op deze logging gehandeld en worden medewerkers aangesproken op hun gebruik van de systemen. Leidend is ook hier dat Fluvium van haar medewerkers verwacht dat zij kunnen uitleggen waarom zij bepaalde persoonsgegevens hebben ingezien.

Deze logging taak ligt bij de, directeur en zal minimaal tweemaal per schooljaar worden uitgevoerd. De Privacy Officer ziet er op toe dat de controle gebeurt, door de directeuren actief te bevragen en zijn bevindingen vast te leggen in een logboek.

Voor stagiairs en tijdelijke medewerkers/zzp'ers is de toegang tot de systemen beperkt. Zij krijgen alleen toegang tot de persoonsgegevens van de eigen klas/leerling waarmee zij te maken hebben. De directeur is verantwoordelijk voor het verstrekken van deze accounts en ziet er op toe dat de deze accounts weer worden ingetrokken na afloop van de stage/werkzaamheden.

Naast het toepassen van dit toegangsbeleid worden de volgende beveiligingsmaatregelen toegepast op systemen waarin persoonsgegevens worden gebruikt:

- Inloggegevens worden verstuurd naar het e-mailadres van de medewerker dat beheerd wordt door (een school van) het bestuur.
- Inloggegevens worden periodiek (minstens 1x per jaar) vernieuwd.
- Er wordt technisch afgedwongen (waar mogelijk) om sterke wachtwoorden te gebruiken.

Bewaartermijnen

Vanuit de privacywetgeving zijn er geen concrete bewaartermijnen voor persoonsgegevens vastgesteld. Wel dient de organisatie hiervoor richtlijnen te hebben. Hierbij is het van belang om na te gaan hoe lang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld. In andere wetten zijn in sommige gevallen wel bewaartermijnen opgenomen waaraan organisaties zich moeten houden.

Het bestuur hanteert mede op basis hiervan de bewaartermijnen voor persoonsgegevens zoals hieronder aangegeven.

Wanneer de bewaartermijn verstreken is moeten de betreffende gegevens vernietigd worden.

Gegevens	**Verplichte bewaartermijn**	**Onderbouwing**
Gegevens over verzuim en afwezigheid	5 jaar nadat een leerling is uitgeschreven	Artikel 9 Bekostigingsbesluit WPO
Gegevens in- en uitschrijving (noodzakelijk voor berekening van bekostiging)	5 jaar nadat een leerling is uitgeschreven	Artikel 9 Bekostigingsbesluit WPO
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school krijgt	7 jaar na afloop van het schooljaar waarop de bekostiging betrekking heeft	Artikel 172 lid 3 WPO
Gegevens in het leerlingdossier	2 jaar nadat een leerling is uitgeschreven en 3 jaar als er sprake is van een verwijzing naar het speciaal onderwijs.	Website Autoriteit Persoonsgegevens
Medische gegevens in het leerlingdossier	n.t.b.	Ligt eraan wie de gegevens verzameld heeft, externe ja/nee

		en de bewaartermijn voor Remedial teaching (rt) laat ruimte voor eigen invulling.
Gegevens met betrekking tot bezwaar-, klachten- of gerechtelijke procedure.	5 jaar nadat leerling is uitgeschreven	
Camerabeelden t.b.v. toezicht	4 weken, tenzij er een incident is vastgelegd.	Website Autoriteit Persoonsgegevens
Gegevens in personeelsdossier met betrekking tot fiscale bewaarplicht	5 jaar na uitdiensttreding	Artikel 52 lid 4 Algemene wet inzake rijksbelastingen
Overige gegevens in het personeelsdossier	2 jaar na uitdiensttreding	
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk door personeel en leerlingen	6 maanden	
Sollicitatiebrief, formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	4 weken zonder toestemming, 1 jaar met toestemming van de sollicitant, 2 jaar na uitdiensttreding voor benoemde collega.	

Afspraken over mobiele devices in bruikleen en privé devices

Het bestuur en/of de school leent afhankelijk van de functie of aard van de werkzaamheden mobiele devices uit aan haar medewerkers. Dit kan gaan om een smartphone, tablet of een laptop. De devices zijn voorzien van beveiliging, zodat gegevens goed beschermd zijn. De devices zijn naast antivirus o.a. voorzien van back-up functionaliteit, encryptie (versleuteling van gegevens) en worden na inname weer opgeschoond.

Aanvullend hierop wil de school nog een aantal afspraken schriftelijk vastleggen over het gebruik van het device wanneer deze in bruikleen wordt gegeven aan een medewerker. Deze afspraken zijn vastgelegd in **bijlage F** van dit handboek.

Gebruik prive-devices
Mobiele devices in eigendom van de medewerker kunnen gebruikt worden voor schoolwerkzaamheden indien ze voorzien zijn van de volgende beveiligingseisen, zodat persoonsgegevens goed beschermd zijn.

- Het device is voorzien van een wachtwoord of code.
- Het device is voorzien van up-to-date software beveiliging.
- E-mail en andere apps of online toepassingen van Fluvium moeten afgeschermd worden met een apart wachtwoord. *Vind je het lastig om meerdere werkgerelateerde wachtwoorden te onthouden? Gebruik dan een wachtwoordkluisje van Last Pass of True key. Daarmee kun je zakelijk en privé op een veilige manier scheiden op je eigen device. En hoef je maar 1 wachtwoord te onthouden.*
- E-mail en andere apps of online toepassingen mogen niet toegankelijk zijn voor andere gebruikers.
- Wachtwoorden van ParnasSys en Raet mogen niet onthouden worden in de browser. *Denk ook hier eens aan wachtwoordkluisjes!*
- Er worden geen bestanden lokaal opgeslagen, maar alleen op de daarvoor aangewezen bewaarplaatsen van Fluvium.
- Wanneer je persoonsgegevens verwerkt mag er geen gebruik gemaakt worden van een openbaar Wifi-netwerk.

Vragen of 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 Fluvium hier een centraal punt voor in hebben gericht: **privacy@stichtingfluvium.nl.** Dit account wordt beheerd door de privacy officer. Hij zal indien nodig overleg hebben met de functionaris gegevensbescherming en/of het college van bestuur.

Wettelijk hebben de personen (betrokkenen) van wie Fluvium persoonsgegevens verzamelen bepaalde rechten. Deze rechten zijn:

- Het recht op dataportabiliteit. Het recht om persoonsgegevens over te dragen.
- Het recht op vergetelheid. Het recht om 'vergeten' te worden.
- Recht op inzage. Dat is het recht van mensen om de persoonsgegevens die u van hen verwerkt in te zien.
- Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die u verwerkt te wijzigen.
- Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken.
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.
- Het recht om bezwaar te maken tegen de gegevensverwerking.

Als je zelf inzage wil 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 om inzage stellen aan jouw leidinggevende.
- ➢ **Een leerling of ouder** die jou deze vraagt stelt, kan je doorverwijzen naar: de betreffende schooldirecteur.

Verwerkersovereenkomsten

In de privacywetgeving is bepaald dat het schoolbestuur als Gegevensverantwoordelijke afspraken moet maken met alle leveranciers van de school die leerlinggegevens verwerken in zogenaamde Verwerkersovereenkomsten. Het gaat hierbij bijvoorbeeld om uitgevers van digitaal lesmateriaal, leveranciers van toetsen, onderwijsadviesdiensten, etc.

Een uitzondering hierop vormt de uitwisseling van gegevens met de overheid (DUO) in het kader van bekostiging of toezicht of het Samenwerkingsverband in het kader van passend onderwijs.

De verwerkersovereenkomsten worden waar mogelijk bovenschools afgesloten. Hiervoor is in een inventarisatie gedaan van de lopende contracten van de scholen binnen het bestuur.

Wanneer een school een contract afsluit met een nieuwe leverancier zal er een nieuwe verwerkersovereenkomst gesloten moeten worden. De school is verplicht om nieuwe contracten door te geven aan het bestuur.

Wanneer het gaat om een leverancier die alleen een contract heeft met een individuele school, is de school zelf verantwoordelijk voor het afsluiten van de verwerkersovereenkomst.
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 **https://www.privacyconvenant.nl**

In **I.Verwerkersovereenkomsten** is een overzicht opgenomen van de leveranciers waar het bestuur op dit moment een verwerkersovereenkomst mee heeft. Voor vragen over het afsluiten van verwerkersovereenkomsten of het doorgeven hiervan, kan men terecht bij de privacy officer via **privacy@stichingfluvium.nl**

Rollen en verantwoordelijkheden

Voor het vaststellen en uitvoeren van het IBP-beleid zijn verschillende rollen en verantwoordelijkheden vastgesteld binnen het bestuur.

Dit handboek is bedoeld om praktische uitvoering te geven aan het IBP-beleid, met name ten aanzien van de organisatorische maatregelen. Voor de technische maatregelen voor informatiebeveiliging en privacy dienen afzonderlijke plannen opgesteld te worden.

De volgende rollen en verantwoordelijkheden zijn bepaald ten aanzien van het vaststellen van de inhoud en (de controle op) de toepassing van dit handboek.

Onderwerp	Verantwoordelijk voor	Rol/functie
Privacyreglement	Vaststellen	GMR met CvB
	Communicatie met ouders	Directeuren
Gebruik beeldmateriaal en online diensten	Toestemming vragen aan ouders en registreren	Directie
Uitwisseling persoonsgegevens	Bepalen met welke partijen persoonsgegevens uitgewisseld mogen worden en op welke wijze.	Bestuurder in overleg met privacy officer
	Toestemming vragen aan ouders en registreren	Directie
Gedragscode	Vaststellen	GMR en CvB
	Bewustwording en toezien op toepassing gedragscode	Directie
	Toepassen gedragscode	Alle medewerkers
	Opstellen en toepassen protocol voor leerlingen	Directie
Document- en datamanagement	Toepassen van technische beveiligingsmaatregelen (backup, encryptie, etc.)	Cloudwise olv de privacy officer
	Vaststellen bewaarplaatsen	Bestuurder
	Vaststellen bewaartermijnen	Bestuurder

	Vernietiging persoonsgegevens conform bewaartermijnen	Directie en personeelszaken
Toegangsbeleid	Verstrekken en intrekken beperkte accounts stagiaires/tijdelijk medewerkers /externen	Directeur
	Periodieke logging en (aan)spreken medewerkers over opvallend gebruik van de systemen Toepassen technische beveiligingsmaatregelen (o.a. automatisch vernieuwen en sterkte wachtwoord)	Privacy officer
Verwerkersovereenkomsten	Doorgeven nieuwe verwerkers (leveranciers) aan bestuurssecretariaat	Directie
	Afsluiten verwerkersovereenkomsten voor meerdere scholen	Privacy officer
	Afsluiten verwerkersovereenkomsten voor individuele scholen	Privacy officer
Datalekken	Protocol vaststellen	Bestuurder
	Datalekken doorgeven aan Meldpunt	Alle medewerkers
	Verzamelen meldingen en benodigde informatie	Privacy officer
	Melden en registreren	Privacy officer
	Afweging maken tot melding Autoriteit Persoonsgegevens	Privacy officer i.o.m. CvB en FG
	Melding maken bij Autoriteit Persoonsgegevens	FG
Devices in bruikleen	Afsluiten gebruikersovereenkomst voor devices die in bruikleen worden gegeven.	Personeelszaken
Handboek Privacy	Controle en toezicht op toepassing handboek	Privacy officer i.c.m. FG

Controle en toezicht

Twee jaarlijks wordt onderstaande (niet uitputtende) controlelijst besproken in het DO om na te gaan of het handboek is geïmplementeerd. De resultaten worden gerapporteerd aan de bestuurder.

#	Maatregelen met betrekking tot privacy en informatiebeveiliging	Ja*/ Nee	Waaruit blijkt dit?
1	Het **privacyreglement** wordt door de school 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.		
5	Het **protocol datalekken** is bij de medewerkers bekend. Men weet wat er van hen verwacht wordt.		
6	**Toegang** tot software en systemen met persoonsgegevens op school wordt voor stagiairs/tijdelijk medewerkers/externen beperkt		
7	De afspraken **over de bewaarplaatsen van gegevens en informatie** (Document- en datamanagement) worden nageleefd.		
8	Er wordt middels een **gedragscode** en een **protocol voor leerlingen** structureel en regelmatig aandacht besteed aan de zorgvuldige verwerking van persoonsgegevens.		
9	Bij **uitdiensttreding** worden alle accounts ingetrokken en apparatuur ingenomen.		
10	Voor alle door de school uitgegeven apparatuur aan medewerkers zijn **gebruikersovereenkomsten** afgesloten.		
11	**Fysieke ruimtes** op school met persoonsgegevens van gevoelige aard (op papier of op server) **zijn beveiligd** tegen onbevoegde toegang.		

Bijlagen

A. Privacyreglement Fluvium

Inleiding

Informatie en ict zijn noodzakelijk in het onderwijs. Omdat we met die informatie en ict ook persoonsgegevens verwerken, is de **Algemene Verordening Gegevensbescherming** (AVG) van toepassing. De AVG bepaalt onder welke voorwaarden persoonsgegevens gebruikt mogen worden en dat er passende technische en organisatorische maatregelen genomen moeten worden om de persoonsgegevens te beschermen.

Stichting Fluvium vindt privacy van haar leerlingen, ouders en medewerkers belangrijk en gaat daarom zorgvuldig om met hun persoonsgegevens.

Dit privacyreglement beschrijft hoe Fluvium omgaat met de verwerkingen van persoonsgegevens en de beveiliging van de informatie. Het is bedoeld als centrale informatiebron voor alle betrokkenen.

Per categorie betrokkenen (leerlingen en hun ouders/verzorgers, personeelsleden, derden) leest u hierin terug om wat voor soort persoonsgegevens het gaat, wat het doel en de grondslag van de verwerking is, wat het toegangs- en beveiligingsbeleid is en in hoeverre de persoonsgegevens met derden worden gedeeld. Ook leest u in dit privacyreglement hoe lang Fluvium persoonsgegevens bewaart en welke rechten u heeft onder de AVG.

Met dit privacyreglement voldoet het bestuur van Fluvium aan de informatieplicht uit de AVG. Het privacyreglement wordt jaarlijks herzien.

1. Privacy van leerlingen en hun ouders

De openbare scholen van Fluvium Openbaar Onderwijs maken actief werk van de veelkleurigheid die onze samenleving kenmerkt. Zij denken niet in 'hokjes' en dragen bij aan democratisch burgerschap. We gaan kinderen voor in het leren van elkaar en het respecteren van diverse culturele, levensbeschouwelijke en economische achtergronden. Wij sluiten niemand buiten.

Op basis van gelijkwaardigheid leren onze kinderen dat iedereen verschillend mag zijn. En dat we daarin blijvend van elkaar leren.

Om deze doelstelling waar te maken is het van belang goed te weten wie deze leerling is, wat zijn of haar 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.

1.1. Om wat voor soort persoonsgegevens gaat het?
Van leerlingen en hun ouders verzamelen wij de volgende categorieën persoonsgegevens:

- NAW- en contactgegevens
- geboortedatum en culturele achtergrond
- hoogst genoten opleiding ouders
- Administratienummer (o.a. BSN)
- ontwikkelingsvoortgang en leerresultaten
- gezondheidsgegevens (bijv. allergieën)
- verzuimgegevens
- administratieve gegevens (bijv. in welke klas uw kind zit, het rooster etc.)
- beeldmateriaal
- gegevens die nodig zijn voor het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten
- loggegevens

1.2. Wat zijn de doelen en grondslagen van de verwerkingen?
De persoonsgegevens worden verzameld om:

- te voldoen aan wettelijke verplichtingen
- leerlingen toe te laten op school
- bekostiging te ontvangen van de overheid
- te communiceren met leerlingen en ouders
- PR-doeleinden
- onderwijs te organiseren
- onderwijs uit te voeren /af te stemmen op de ontwikkeling van de leerling
- leerlingen extra ondersteuning/begeleiding te bieden
- administratie- en financieel beheer doeleinden
- de systemen te beveiligen, controleren en misbruik/oneigenlijk gebruik te voorkomen
- De continuïteit en goede werking van de systemen te waarborgen

De persoonsgegevens van leerlingen worden verzameld op grond van een wettelijke verplichting, de toestemming van ouders/verzorgers (bijv. de verwerking van beeldmateriaal) of op grond van de noodzakelijkheid van die persoonsgegevens voor het vervullen van Fluviums onderwijstaak.

1.3. Toegang en beveiliging
Binnen Fluvium zijn de medewerkers bewust van de privacy van leerlingen. Fluvium vertrouwt daarom in eerste instantie op de integriteit van haar medewerkers om niet de persoonsgegevens van leerlingen in te zien waar ze in hun werk niet mee te maken hebben.

Om op de toegang van persoonsgegevens te controleren en oneigenlijk gebruik te voorkomen, worden de loggegevens periodiek gecontroleerd. Bij opvallend gebruik van de systemen worden medewerkers daarover (aan)gesproken.

Voor stagiairs, tijdelijke medewerkers en externen wordt de toegang tot de systemen beperkt tot de eigen klas/leerlingen. De accounts worden weer ingetrokken na afloop van de stage/tijdelijke werkzaamheden.

Met de leverancier van ParnasSys is een zogenaamde verwerkersovereenkomst (conform het model van de PO-raad) afgesloten, waarin o.a. afspraken zijn gemaakt over beveiliging en back-up van de data die in ParnasSys wordt opgeslagen. ParnasSys voldoet aan de nationale standaarden op het gebied van beveiliging die de overheid heeft bepaald. Als de school gegevens moet uitwisselen met andere scholen of de overheid, dan gebeurt dit via het beveiligde ParnasSys.

Eventuele papieren dossiers die persoonsgegevens van leerlingen bevatten, worden in afgesloten kasten bewaard.

Voor digitale leermiddelen en toetsen worden systemen van diverse leveranciers of uitgeverijen gebruikt. Met deze partijen zijn eveneens verwerkersovereenkomsten afgesloten. Daarmee verplichten leveranciers/uitgeverijen zich onder meer te voldoen aan de nationale standaarden en voorzieningen met betrekking tot de veilige uitwisseling van persoonsgegevens. Op termijn wordt bovendien gebruik gemaakt van de ECK-ID die het mogelijk maakt om alleen nog maar gepseudonimiseerde gegevens met deze partijen uit te wisselen. Meer informatie hierover is hier te vinden.

1.4 Worden de persoonsgegevens met derden gedeeld?
De persoonsgegevens van leerlingen worden **niet** met derden gedeeld zonder toestemming van de ouders, tenzij de school wettelijk verplicht is om bepaalde persoonsgegevens te verstrekken.

Zo heeft de school bijvoorbeeld wettelijke verplichtingen om persoonsgegevens te delen met het samenwerkingsverband, de Inspectie, leerplichtambtenaar, DUO enz.

De meest voorkomende gevallen waarin de school toestemming aan ouders vraagt om persoonsgegevens met derden te delen, zijn de situaties waarin de school een externe expert wil benaderen voor aanvullende onderwijs- en zorgbegeleiding voor de leerling. Denk aan een schoolmaatschappelijk werker, schoolarts, orthopedagoog, ambulant begeleider, remedial teacher. Toestemming van ouders wordt schriftelijk gevraagd en opgeslagen in het leerlingdossier.

2. Privacy van medewerkers

2.1. om wat voor soort persoonsgegevens gaat het?
Van medewerkers verzamelen wij de volgende categorieën persoonsgegevens:

- NAW- en contactgegevens;
- Persoonsgegevens die op het identiteitsbewijs staan
- Salarisgegevens waaronder IBAN
- Gegevens over functioneren, loopbaan en benoeming
- Gegevens over een evt. justitieel verleden
- Verzuim- en verlofgegevens

- Gegevens over de klas waaraan een medewerker gekoppeld is

- Loggegevens over het gebruik van de systemen

2.2. Wat zijn de doelen en grondslagen voor de verwerkingen?

Deze gegevens worden verzameld om:
- Personeel aan te nemen en te ontslaan
- Leiding te geven
- Te voldoen aan (fiscaal) wettelijke verplichtingen
- Personeelsadministratie en -beleid te voeren
- Loon uit te betalen
- Medewerkers bij te kunnen scholen
- Interne controle en bedrijfsvoering
- Personeel toegang te geven tot het leerlingvolgsysteem met bijbehorende autorisaties
- Personeel te laten werken met digitale onderwijsmiddelen
- de systemen te beveiligen, controleren en misbruik/oneigenlijk gebruik te voorkomen
- De continuïteit en goede werking van de systemen te waarborgen

De persoonsgegevens worden verzameld op de grondslag van een wettelijke verplichting, het uitvoeren van een overeenkomst of toestemming van medewerkers.

2.3. Toegang en beveiliging

Medewerkers kunnen hun eigen digitale personeelsdossier inzien met behulp van hun eigen inlog. Binnen Fluvium zijn medewerkers zich bewust van elkaars privacy..
Voor personeelsgegevens die in dezelfde systemen worden verwerkt als die van leerlingen, gelden dezelfde beveiligingsmaatregelen uit paragraaf 1.3.

2.4. Worden de persoonsgegevens met derden gedeeld?

Binnen Fluvium delen wij persoonsgegevens van medewerkers **niet** met derden zonder toestemming van de betreffende medewerker, tenzij de school wettelijk verplicht is om bepaalde persoonsgegevens te verstrekken.

3. Privacy van derden
In deze categorie gaat het om vrijwilligers, sollicitanten, extern ingehuurd personeel en oud-leerlingen.

3.1. om wat voor soort persoonsgegevens gaat het?

- NAW- en contactgegevens
- Betaalgegevens
- Gegevens over een eventueel justitieel verleden
- Studie- en loopbaangegevens
- Persoonsgegevens op het ID-bewijs (in geval van een externe professional)

3.2. Wat zijn de doelen en grondslagen voor de verwerkingen?

Deze gegevens worden verzameld om:

- De geschiktheid van een sollicitant te beoordelen
- De veiligheid binnen de organisatie te borgen
- De door de sollicitant gemaakt onkosten af te handelen
- Inkomende facturen te betalen
- Externen toegang geven tot ICT en software die nodig zijn bij het uitvoeren van hun taak
- Te voldoen aan wettelijke verplichtingen
- Te communiceren met vrijwilligers, oud-leerlingen en hun ouders, externe professionals

3.3 Toegang en beveiliging

Binnen Fluvium zijn medewerkers privacybewust en is het niet de bedoeling dat persoonsgegevens van derden worden geraadpleegd zonder dat dit te maken heeft met je werk. Aan de hand van periodieke logging wordt opvallend gedrag gedetecteerd en kunnen medewerkers zo nodig hierop worden aangesproken. Medewerkers weten dat hun gebruik van de systemen wordt gecontroleerd.

3.4 worden de pgg met derden gedeeld?

De persoonsgegevens van sollicitanten worden alleen verstrekt aan externe partijen die namens het bestuur een test of assessment verzorgen. In dat geval worden slechts die persoonsgegevens verstrekt die noodzakelijk zijn voor de test of assessment.

Deze gegevens van externen worden verstrekt aan uitzendbureaus en detacheringsbureaus waarmee het bestuur samenwerkt.

Gegevens van vrijwilligers en oud-leerlingen of hun ouders worden niet met derden gedeeld.

4. Bewaartermijnen

Gegevens	Bewaartermijn
Gegevens over verzuim en afwezigheid	5 jaar nadat een leerling is uitgeschreven
Gegevens in- en uitschrijving (noodzakelijk voor berekening van bekostiging)	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
Gegevens in het leerlingdossier	2 jaar nadat een leerling is uitgeschreven
Gegevens met betrekking tot bezwaar-, klachten- of gerechtelijke procedure.	5 jaar nadat leerling is uitgeschreven
Camerabeelden t.b.v. toezicht	4 weken, tenzij er een incident is vastgelegd.
Gegevens in personeelsdossier met betrekking tot fiscale bewaarplicht en loonbelasting	10 jaar na uitdiensttreding
Overige gegevens in het personeelsdossier	2 jaar na uitdiensttreding
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk door personeel en leerlingen	6 maanden
Sollicitatiebrief, formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	4 weken zonder toestemming, 1 jaar met toestemming van de sollicitant, 2 jaar na uitdiensttreding voor benoemde collega.

5. Rechten van betrokkenen

De AVG geeft ouders, medewerkers en andere betrokkenen het recht op inzage in en aanpassing/verwijdering van hun persoonsgegevens. Ook hebben zij recht op beperking van de verwerking van hun persoonsgegevens, het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens en het recht om de digitale persoonsgegevens te ontvangen die

Fluvium van hen heeft. Heeft u toestemming gegeven voor een bepaalde verwerking van persoonsgegevens, zoals toestemming voor het gebruik van beeldmateriaal van uw kind? Dan mag u deze toestemming te allen tijde weer intrekken.

U kunt uw rechten uitoefenen door een e-mail te sturen naar de Functionaris Gegevensbescherming (FG). De contactgegevens staan hieronder. De FG zal uw verzoek binnen de wettelijke termijn afhandelen voor zover dit redelijkerwijs mogelijk is.

Heeft u verder nog een vraag, wilt u een overzicht opvragen van de leveranciers/uitgeverijen met wie Fluvium een verwerkersovereenkomst heeft afgesloten of vindt u dat het privacyreglement niet op de juiste wijze wordt nageleefd binnen het bestuur? Dan mag u natuurlijk ook een e-mail sturen. Als u niet tevreden bent over de reactie van het bestuur, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens.

6. Contactgegevens

Stichting Fluvium Openbaar Onderwijs
KVK 11063129
De Panoven 29
4191 GW Geldermalsen
FG: privacy@stichtingfluvium.nl

B. 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 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.

Wil je meer weten over hoe wij met uw gegevens omgaan?
Kijk dan verder bij:

- Hoe wij met uw gegevens omgaan [link naar onderstaande tekst]
- Privacyreglement [link naar privacyreglement]
- Privacy van leerlingen en hun ouders [link naar onderdeel privacyreglement]
    - Privacy van medewerkers [link naar onderdeel privacyreglement]
    - Privacy van derden [link naar onderdeel privacyreglement]
    - Rechten van betrokkenen [link naar onderdeel privacyreglement]
    - Bewaartermijnen [link naar onderdeel privacyreglement]
    - Contactgegevens [link naar onderdeel privacyreglement]
- Responsible disclosure [link naar bijlage C]

Hoe wij met uw gegevens omgaan
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 voor de juiste begeleiding van een leerling, zoals gezondheidsgegevens (denk aan dyslexie of ADHD).
De leerlinggegevens worden opgeslagen in ons (digitale) administratiesysteem ParnasSys. Dit programma is beveiligd.

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.

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

C. Tekst voor op de website (Responsible disclosure)

Bij Fluvium vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.
Wij vragen je een bijdrage te leveren aan de veiligheid van ict-systemen en het beheersen van de kwetsbaarheid van ict-systemen. Dat kun je doen door de door jou ontdekte kwetsbaarheden op verantwoorde wijze bij Fluvium te melden. Als je een zwakke plek in één van onze systemen hebt gevonden horen wij dit graag zo snel mogelijk, zodat we aanvullende (beveiligings)maatregelen kunnen treffen.

Wij vragen je:

- Je bevindingen te melden via **privacy@stichtingfluvium.nl**.
- De door jou ontdekte kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of (persoons)gegevens van derden in te kijken, te verwijderen of aan te passen.
- Je bevinding/probleem niet met anderen te delen totdat de kwetsbaarheid is verholpen en alle (vertrouwelijke) gegevens die zijn verkregen door de kwetsbaarheid direct na het verhelpen daarvan te wissen.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden.
- Voldoende informatie te geven om de kwetsbaarheid te reproduceren zodat wij deze zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wij zeggen toe dat:

- We reageren zo spoedig mogelijk op jouw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Als je je aan bovenstaande voorwaarden houdt, wij geen aangifte van een strafbaar feit zullen doen of andere juridische stappen tegen je ondernemen betreffende de melding.*
- Wij jouw melding vertrouwelijk behandelen en je persoonsgegevens zonder jouw toestemming niet zullen delen met derden of verder zullen verwerken, tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk.
- Wij je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid.
- In berichtgeving over de gemelde kwetsbaarheid wij je, indien je dit wenst, zullen vermelden als ontdekker van de kwetsbaarheid. Wij streven ernaar alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

* Let op: het feit dat Fluvium geen aangifte tegen jou zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar jouw handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.

D. Toestemmingsformulier

Binnen Fluvium wordt dit toestemmingsformulier toegepast bij de aanmelding.

Toelichting in het kader van privacywetgeving
De gegevens die u heeft ingevuld op het inschrijfformulier, worden opgeslagen in de leerlingadministratie van onze school. Uiteraard worden deze gegevens vertrouwelijk behandeld. Op onze administratie is de Alegemene Verordening Gegevensbescherming van toepassing.
Dit betekent onder andere dat de gegevens door ons worden beveiligd, en dat de toegang tot de gegevens is beperkt tot alleen die medewerkers die de gegevens strikt noodzakelijk nodig hebben bij de uitoefening van hun taak. U heeft als ouder het recht om de door ons geregistreerde gegevens in te zien (voor zover die informatie betrekking heeft op uw kind). Als de gegevens niet kloppen, dan mag u van ons verwachten dat wij – op uw verzoek - de informatie verbeteren of aanvullen.
Een aantal vragen in dit inschrijfformulier zijn wij wettelijk verplicht aan u te stellen. Zo vragen wij naar uw opleidingsniveau. Dit heeft te maken met de wettelijke 'gewichtenregeling': het aantal leerkrachten aan onze school is mede afhankelijk van het totaal van het 'leerlinggewicht' van onze leerlingen. Voor meer informatie over de omgang met de privacy van uw kind(eren), verwijzen wij u naar ons privacyreglement [link].

Toestemming
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.

Foto- en videomateriaal
Op onze school laten wij u met foto's en video's zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Ook uw zoon/dochter kan op deze foto's (en soms in video's) te zien zijn. Graag willen we daarom uw toestemming voor het gebruik van beeldmateriaal van uw zoon/dochter. Uw toestemming geldt alleen voor foto's en video's die door ons, of in onze opdracht worden gemaakt. Het kan voorkomen dat andere ouders foto's maken tijdens schoolactiviteiten die buiten de school plaatsvinden. De school heeft daar geen invloed op. Wij vragen daarom aan ouders om terughoudend te zijn met het maken van foto's en video's en deze niet te delen via sociale media.

Adressenlijst
Op onze school wordt er, per klas, een lijst gemaakt met de adressen van leerlingen. Deze lijst met contactgegevens is erg praktisch om te overleggen met andere ouders, als de kinderen (buiten schooltijd) willen afspreken of als er vragen zijn rondom school, overblijf, etc. Wij vragen hierbij uw toestemming om de naam van uw kind, diens adres en uw telefoonnummer te mogen delen met de andere ouders van de school. Als u er bezwaar tegen heeft, wordt de naam van uw kind niet gedeeld. Deze informatie op de klassenlijst mag uitsluitend gebruikt worden voor persoonlijk gebruik onderling, en dus niet voor bijvoorbeeld reclame.

Online diensten
Online diensten spelen een belangrijke rol in het leven van leerlingen en onderwijzend personeel. Het gebruik van online diensten is onderdeel van het gedrag van leerlingen binnen de school. Online diensten kunnen helpen om het onderwijs te verbeteren en de lessen leuker te maken en om contact te onderhouden met vrienden of klasgenoten. Maar online diensten brengen ook risico's met zich mee, zoals pesten en het ongewild delen van foto's of andere gegevens. Op school besteden we in ons lesprogramma hier aandacht aan. Voor het gebruik van online diensten door uw kind(eren), vragen wij uw toestemming.

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

1 foto's en video's WEL gebruikt mogen worden:

- ☐ op het ouderportaal van de school
- ☐ in de (digitale) nieuwsbrief
- ☐ in de schoolkalender
- ☐ in de schoolgids
- ☐ op de website van de school
- ☐ in folders en flyers ter promotie van de school
- ☐ op sociale-media accounts van de school (Whatsapp, Twitter, Facebook)
  (kruis aan waar u toestemming voor geeft)

2. haar/zijn naam, adres en telefoonnummer WEL / NIET * gedeeld mag worden met andere ouders

3. hij/zij onder schooltijd WEL / NIET * gebruik mag maken van online diensten t.b.v. onderwijsdoeleinden

(* streep door wat niet van toepassing is)

	Ouder/verzorger 1	Ouder/verzorger 2
Naam:		
Datum:		
Plaats:		
Handtekening:		

Toestemmingsformulier uitwisseling derden

De ouders/verzorgers van (*doorstrepen wat niet van toepassing is)*

_____ (*Naam leerling)*

Geven toestemming aan: _____ (*Naam school)*

om de volgende gegevens: _____

te verstrekken aan: _____ (*Naam school/ instantie*)

Voor de volgende doeleinde(n): _____

_____

_____

	Ouder/verzorger 1	Ouder/verzorger 2
Naam:		
Datum:		
Plaats:		

E. Procedure datalekken

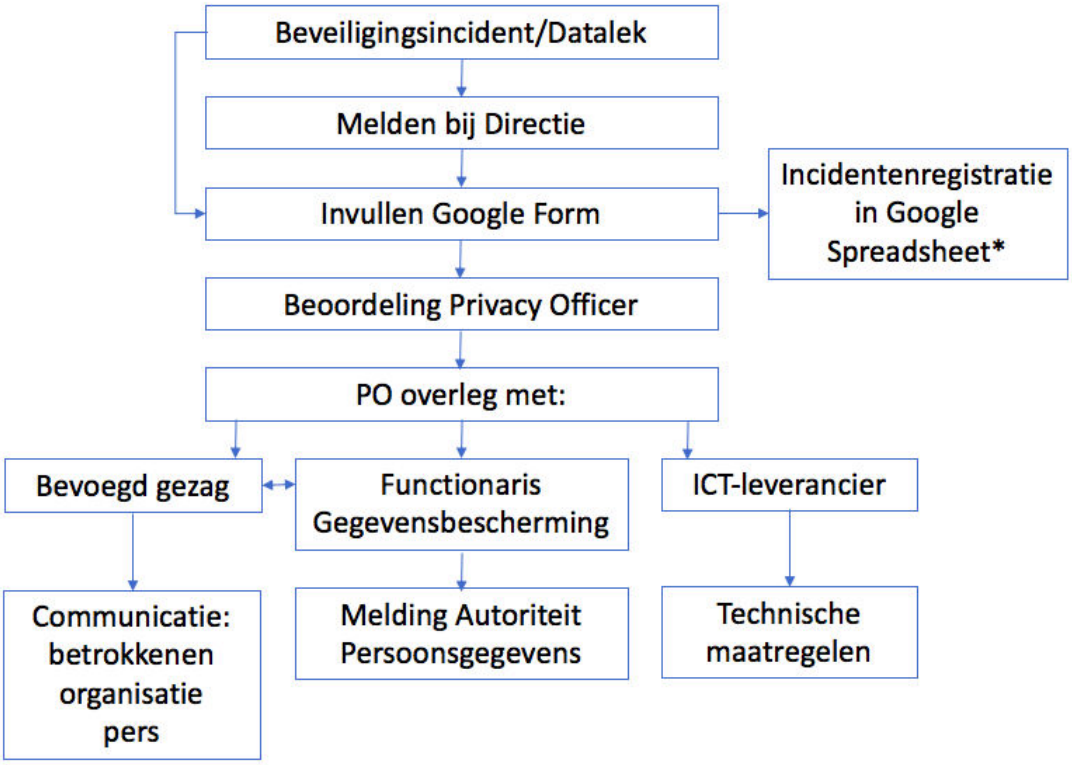
Inleiding

Deze procedure maakt integraal onderdeel uit van het privacybeleid van ons bestuur en is vastgesteld door het college van bestuur.

De procedure bestaat uit 4 onderdelen voor afzonderlijke doelgroepen, te weten:

a. Medewerkers en leerlingen (meldingen aan directeur en/of invullen meldingsformulier beveiligingsincident en datalekken)
b. Directeur (meldingen aan bovenschoolse Privacy Officer)
c. Privacy Officer (registreren en beoordelen melding) en Functionaris Gegevensbescherming (meldingen aan Autoriteit Persoonsgegevens)
d. College van Bestuur (informeren betrokkenen)

Hieronder is de procedure datalekken schematisch weergegeven. Deze wordt op de volgende pagina's verder uitgewerkt.



** Input voor jaarlijkse IBP risicoanalyse*

Er wordt periodiek (minstens één keer per jaar) gecontroleerd of deze procedure, inclusief de onderstaande beschreven stappen, adequaat is geïmplementeerd.

Waarom deze procedure?
Beveiligingsincidenten kunnen leiden tot informatie en/of gegevens die verloren gaan of onbedoeld gewijzigd worden. Dit kan gevolgen hebben voor de kwaliteit en continuïteit van het onderwijs.

Daarnaast kunnen vertrouwelijke gegevens door beveiligingsincidenten op straat komen te liggen of in verkeerde handen vallen. Voor de verwerking van persoonsgegevens zijn regels vastgelegd in de Algemene Verordening Gegevensbescherming (AVG). Het niet zorgvuldig omgaan met vertrouwelijke gegevens kan leiden tot boetes en imagoschade.

Als een beveiligingsincident betrekking heeft op persoonsgegevens, moet er mogelijk binnen 72 uur melding worden gemaakt aan de Autoriteit Persoonsgegevens (voorheen College bescherming persoonsgegevens).

Definities
Wat is een beveiligingsincident?
Een beveiligingsincident is een gebeurtenis waarbij gegevens:

1. verloren zijn geraakt
2. gestolen zijn
3. beschadigd zijn
4. onbedoeld gewijzigd zijn
5. onrechtmatig toegankelijk zijn voor derden

Wat is een datalek?
Er is sprake van een datalek als er bij een opgetreden beveiligingsincident persoonsgegevens betrokken zijn.

Wat zijn persoonsgegevens?
Alle gegevens die (evt. gecombineerd met andere gegevens) tot een persoon herleid kunnen worden.

Voorbeelden persoonsgegevens

- Naam
- BSN
- Pasfoto
- Geboortedatum
- Adres
- IP-adres
- Etc.

Deel A. Medewerkers en leerlingen

Onderstaande teksten zijn opgenomen op de website, schoolgids en/of intranet van de scholen binnen ons bestuur.

Persoonsgegevens gelekt? Meld ze direct!

Als er sprake is van gestolen computers, opslagmedia of (papieren) documenten, virussen of kwijtgeraakte logingegevens waardoor persoonsgegevens toegankelijk zijn voor anderen, meld dit dan zo snel mogelijk via privacy@stichtingfluvium.nl of bij de schoolleiding van de school.

Op deze manier hopen we op <naam school> veilig en zorgvuldig om te gaan met gegevens van onze leerlingen, hun ouders en onze medewerkers. Klik **hier** voor meer informatie over hoe wij omgaan met privacy en zorgen voor een veilig schoolklimaat.

Nog 3 belangrijke tips:

- Deel je logingegevens nooit met anderen en laat ze niet meekijken.
- Als je een link in je mail niet vertrouwt, klik er dan niet op.
- Mocht je computer besmet zijn met een virus, sluit de computer dan zo snel mogelijk af en verbreek de internet- of netwerkverbinding, om

Voorbeelden beveiligingsincident

- computer of software die niet werkt of bruikbaar is
- kwijtgeraakte USB-stick
- gestolen laptop
- inbraak door een hacker
- DDOS aanval
- malware- of virusbesmetting
- gestolen logingegevens
- onbeveiligde serverruimte
- leerlinglijst met adres-gegevens in het museum laten liggen
- notulen van een zorgoverleg in de teamkamer laten liggen

Deel B. Directeur

Stap 1 - Analyseer en beoordeel (binnen 8 uur na melding)

Heeft de melding betrekking op persoonsgegevens?
Meld dit direct via privacy@stichtingfluvium.nl bij de privacyfunctionaris binnen ons bestuur.

> Wat is een datalek?
>
> Er is sprake van een datalek als er bij een opgetreden beveiligingsincident Persoonsgegevens betrokken zijn.

Is er sprake van opzettelijk misbruik of strafbare feiten, zoals diefstal, hacken of DDOS?
Neem (ook) contact op met de schooldirecteur in verband met te nemen sancties en/of het doen van aangifte.

Stap 2 - Inventariseer en registreer

Indien er een melding wordt gedaan van een beveiligingsincident, dan worden de volgende gegevens geregistreerd:

Naam:
Datum:
Tijdstip:
Omschrijving incident:
Soort gegevens:
Omvang gegevens: (aantal personen)
Betrokkenen:
Locatie:
Type hardware (tagcode):
Naam software:

Prioriteit: (indien datalek: hoog)
Back-up aanwezig?: ja/nee
Zijn de gegevens geëncrypt?: ja/nee

Stap 3 – Neem herstelmaatregelen in overleg met de ICT-er

Is er sprake van diefstal, verlies of beschadiging?
Dan moet het systeem vervangen worden en/of de back-up teruggeplaatst worden (indien aanwezig). Neem hiervoor contact op met de ict-leverancier van de school.

Is er sprake van onrechtmatige toegang?
Dan dient de toegang afgesloten te worden door fysieke beveiliging, een wijziging in de configuratie van het netwerk of in de accounts van computers, netwerkapparatuur of applicaties, zoals wachtwoorden. Pas dit zelf aan de software of neem hiervoor contact op met de ict-leverancier van de school.

Is er sprake van DDOS aanval op servers die in beheer zijn van de school?
Dan dient relevante netwerk apparatuur afgesloten of opnieuw geconfigureerd te worden, eventueel in overleg met leveranciers of externe beheerders. Neem hiervoor contact op met de ict-leverancier van de school of de leverancier van het betreffende softwarepakket.

Is er sprake van malware of anti-virus aanvallen?
Dan dient de computer of apparatuur uit het netwerk genomen, opgeschoond en hersteld te worden. Indien nodig dienen back-ups teruggeplaatst te worden. Neem hiervoor contact op met de ict-leverancier van de school.

Stap 4 – Neem preventieve maatregelen en registreer deze bij de melding

De melding kan pas afgesloten worden als de herstelmaatregelen zijn uitgevoerd en er preventieve maatregelen zijn genomen en beschreven om het risico op toekomstige incidenten te vermijden of te verkleinen.

De herstelmaatregelen en preventieve maatregelen worden geregistreerd bij de melding.

N.B. De registratie van meldingen wordt meegenomen in de periodieke evaluatie van het privacybeleid van ons bestuur. In de evaluatie wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Deel C. Privacy Officer en Functionaris Gegevensbescherming

Dit onderdeel is opgenomen in het procedurehandboek van de bovenschoolse Privacyfunctionaris. Dit betreft een rol die op bovenschools niveau is belegd en belast is met onder andere de volgende taken en verantwoordelijkheden:

- (Laten) uitvoeren risicoanalyses
- (Laten) opstellen / bijwerken beleidsplan
- (Laten) opstellen, evalueren en controleren jaarplan
- Rapporteren (relevante) incidenten en datalekken aan directeur/bestuurder

Stap 1 - Controleer en registreer

Controleer of al gegevens zijn geregistreerd over het beveiligingsincident. Vul deze registratie aan met de informatie die uit de volgende stappen naar voren komt.

Stap 2 – Bepaal of er sprake is van een datalek (binnen 8 uur na melding)

Zijn er bij het incident persoonsgegevens verloren gegaan?
Er is geen kopie of back-up aanwezig van de persoonsgegevens

Is er bij het incident sprake van onrechtmatige verwerking van persoonsgegevens? En kan dit niet uitgesloten worden?
Onbevoegden hebben onrechtmatig toegang kunnen krijgen tot de persoonsgegevens

Indien Ja op één van beide → Ga naar stap 3
Indien Nee op beide →Er is geen sprake van een datalek, overleg met systeembeheer over preventieve maatregelen

N.B. Schakel indien nodig een externe deskundige in en informeer de betrokken leverancier(s)! Zie bewerkersovereenkomst voor de afspraken in het kader van datalekken met leveranciers.

Stap 3 – Afweging meldplicht i.s.m. functionaris gegevensbescherming (FG)

Bepaal of er sprake is van meldplicht
Zijn er persoonsgegevens van gevoelige aard gelekt of leidt de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

Indien Ja → Ga naar stap 4
Indien Nee → Er is geen sprake van meldplicht, overleg met systeembeheer over preventieve maatregelen

Gegevens van gevoelige aard:
Godsdienst of levensovertuiging, ras, politieke gezindheid, ras, gezondheid, seksuele leven, lidmaatschap vakvereniging, strafrechtelijke gegevens of over onrechtmatig of hinderlijk gedrag, financiële gegevens of over de economische situatie, gegevens die kunnen leiden tot stigmatisering (schoolprestaties, relatieproblemen), gebruikersnamen en wachtwoorden, gegevens die kunnen worden gebruikt bij identiteitsfraude (BSN)

Nadelige gevolgen:
Misbruik in het criminele circuit van grote databestanden, ingrijpende beslissingen die op basis van (gewijzigde) gegevens worden genomen, gevolgen die binnen ketens van gegevensverwerking kunnen optreden.

Stap 4 – Informeer het college van bestuur en bepaal of betrokkenen ook geïnformeerd dienen te worden.

Ontbreken er technische beschermingsmaatregelen waardoor het datalek (waarschijnlijk) nadelige gevolgen kan hebben voor leerlingen, ouders of medewerkers?
De gegevens zijn niet voorzien van encryptie of de encryptie is verouderd.

Indien Ja → Ga naar de volgende vraag
Indien Nee → Ga naar stap 5 en informeer het college van bestuur

Zijn er zwaarwegende redenen om de melding aan leerlingen, ouders of medewerkers achterwege te laten?
Het informeren van de leerlingen, ouders of medewerkers kan negatieve gevolgen hebben voor de veiligheid van anderen.

Indien Ja → Ga naar stap 5 en informeer het college van bestuur
Indien Nee → Ga naar stap 5 en informeer het college van bestuur en de communicatiemedewerker (zie deel D procedure Melden beveiligingsincidenten en datalekken)

Stap 5 – Meld het datalek bij de Autoriteit (binnen 72 uur na melding) voor FG?!

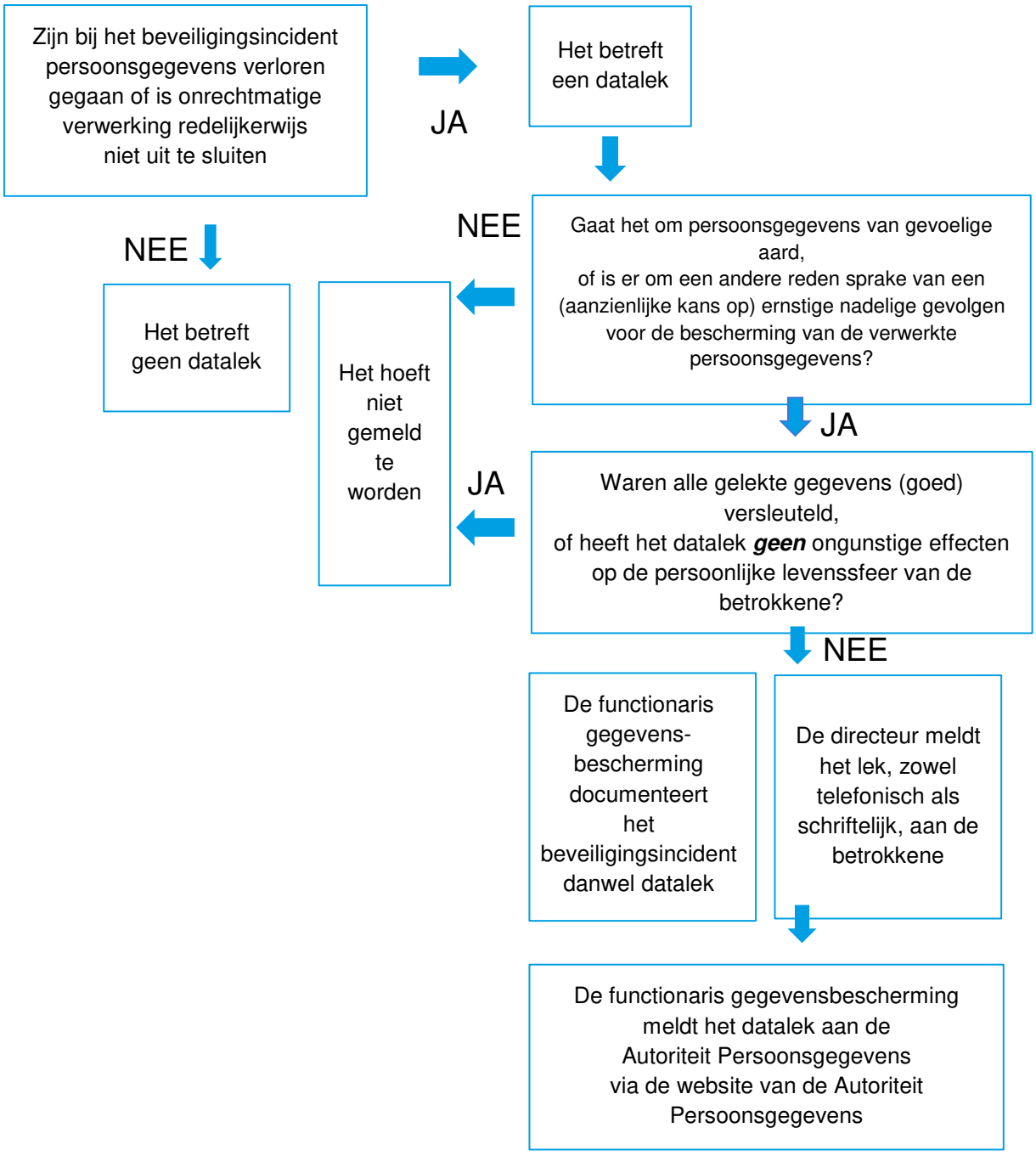
Verzamel alle benodigde informatie (zie bijlage A voor vragenlijst)

Na toestemming van het college van bestuur wordt door de functionaris gegevensbescherming een melding gedaan via **http://datalekken.autoriteitpersoonsgegevens.nl** of (indien de website niet beschikbaar is) via faxnummer 070 - 888 85 01

De melding wordt minimaal 3 jaar bewaard. Informeer indien nodig de leverancier over de melding.

Onderstaand beslismodel kan worden gebruikt om te achterhalen of zich een datalek heeft voorgedaan en of dit moet worden gemeld.

De functionaris gegevensbescherming overlegt met de bestuurder:



Deel D. Bevoegd Gezag

Informeer de betrokkenen (binnen 1 week na melding) via de daarvoor vastgestelde communicatiemiddelen indien er sprake is van een datalek.

Het bevoegd gezag wordt van een datalek op de hoogte gesteld door de Privacy Officer. Deze verstrekt ook de benodigde gegevens ten behoeve van de communicatie.

In de kennisgeving aan de betrokkene wordt in ieder geval vermeldt:
Een algemene omschrijving van de aard van het incident, de contactgegevens om meer informatie over de inbreuk te verkrijgen, en de maatregelen die genomen zijn en/of door betrokkene genomen moeten worden om negatieve gevolgen te beperken.

Bij grootschalige datalekken dient er ook een persbericht in overleg met het bevoegd gezag opgesteld te worden.

F. Model Gebruikersovereenkomst

De werkgever: Fluvium

En de werknemer:
< Naam >
< Geboortedatum >
< Adres >

Verklaren dat zij een gebruikersovereenkomst mobiele telefonie of laptop/device voor onbepaalde duur zijn aangegaan, in aanmerking nemende dat:

- werkgever aan werknemer een mobiele telefoon of laptop/device (hierna: de apparatuur) heeft verstrekt ten behoeve van de uitoefening van de werkzaamheden van de dienstbetrekking;
- de apparatuur eigendom is van werkgever en in bruikleen wordt gegeven aan werknemer;
- deze overeenkomst de nadere gebruiksvoorwaarden bepaalt waaronder werknemer de apparatuur kan gebruiken.

1. Aard en uitvoering
Het type apparatuur en het abonnement worden door werkgever vastgesteld en aangeschaft.

2. Rechten en plichten van werknemer
a) Werknemer verklaart de apparatuur in goede staat te hebben ontvangen en zal deze niet aan derden ter beschikking stellen, verpanden noch op enige andere wijze vervreemden.
b) Werknemer is verantwoordelijk voor het in goede en representatieve staat houden van de apparatuur.
c) Het is werknemer verboden de apparatuur te gebruiken voor activiteiten die in strijd zijn met de bedrijfsdoelstellingen of het imago van werkgever kunnen schaden.

3. Gebruik van de apparatuur door werknemer
De werknemer wordt voor de uitoefening van de dienstbetrekking een mobiele telefoon ter beschikking gesteld met abonnement die hij hoofdzakelijk voor zakelijke doeleinden dient te gebruiken.

4. Gebruik van de apparatuur in de auto
Het is werknemer verboden te telefoneren in de auto zonder gebruikmaking van een carkit dan wel een handsfreeset. Niet handsfree bellen zal onder alle omstandigheden worden aangemerkt als bewust roekeloos handelen. Werkgever zal geen aansprakelijkheid aanvaarden voor zaak- of letselschade als gevolg hiervan, tevens zijn boeten voor rekening van werknemer.

5. Termijn van gebruik, beëindiging dienstverband en functieverandering
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.

6. Diefstal en beschadiging
a) Werknemer dient alle zorgvuldigheid in acht te nemen ter voorkoming van beschadiging, diefstal of verlies van de apparatuur.
b) In geval van schade of diefstal van de apparatuur is werknemer verplicht dit zo spoedig mogelijk, doch uiterlijk binnen 24 uur bij werkgever te melden. Werknemer dient verder het gebruik onmiddellijk te laten blokkeren via de klantenservice van de provider of de interne contactpersoon. Als contractant draagt werkgever het risico voor misbruik na diefstal, mits aan het hiervoor gestelde is voldaan.
c) Werknemer kan aansprakelijk worden gesteld voor schade aan de apparatuur ontstaan door verwijtbare nalatigheid of onachtzaamheid.

7. Bewustzijn
a) Werknemer is op de hoogte dat werkgever informatie omtrent het gebruik van de mobiele telefoon kan aanleveren aan de werkgever.
b) Werknemer verklaart zich akkoord dat, indien gehandeld in strijd met de bepalingen van deze gebruikersovereenkomst mobiele telefonie, de naheffingsaanslagen loonheffing en een bedrag ter grootte van de correctie nota's werknemersverzekeringen inclusief eventuele boetes en rente die als gevolg van dit handelen worden opgelegd aan werkgever, zullen worden verhaald op werknemer.
c) Door ondertekening van deze overeenkomst verklaart werknemer dat hij gevolgen van deze overeenkomst en het onderliggende beleid mobiele telefonie heeft begrepen en zich daarmee akkoord verklaart.

Aldus overeengekomen en getekend te <plaats>, <datum>.

Fluvium
Namens deze:

<ondertekening werknemer> <ondertekening werkgever>

G. Cameratoezicht

In het belang van de veiligheid, de gezondheid en het welzijn van leerlingen en medewerkers zijn kunnen scholen ervoor kiezen om camera's op te hangen. Met het cameratoezicht worden de volgende doelen nagestreefd:

- Bewaking in verband met toegang, schade door vandalisme en diefstal
- Herkenning of identificatie van personen die bij gebeurtenissen betrokken zijn geweest
- Bevorderen van het gevoel van veiligheid
- Preventief, ter voorkoming van onwenselijk gedrag
- Ondersteuning bij opsporing van strafbare feiten

Informatievoorziening
De camera's zijn zichtbaar opgehangen, er wordt in principe geen gebruik gemaakt van verborgen camera's. In bijzondere gevallen, bij vermoeden van onrechtmatig handelen van leerlingen of personeel, kan tijdelijk een verborgen camera worden geplaatst.

Bij het betreden van de school wordt gewaarschuwd dat er cameratoezicht wordt uitgevoerd.

Bewaartermijn beelden

- De camerabeelden worden maximaal 4 weken bewaard behoudens voor de beelden van de incidenten die in behandeling zijn. Indien er in de periode geen incidenten hebben plaatsgevonden of zijn gemeld bij de schoolleiding worden de beelden verwijderd.
- Bij geconstateerde incidenten worden de daaraan te relateren camerabeelden pas verwijderd nadat het incident is afgehandeld. Camerabeelden die gebruikt worden in het kader van onderzoek, waarvan aangifte is gedaan bij de politie, worden pas vernietigd na overleg met de politie. De termijn van vier weken is in deze gevallen niet van toepassing.
- Incidenten die het bewaren van beelden noodzakelijk maken, worden geregistreerd en gedocumenteerd in een logboek. Als beelden van een incident worden bekeken, wordt daarvan melding gemaakt in een logboek. Het logboek wordt beheerd door de systeembeheerder.

Bekijken van beelden
Toestemming voor het bekijken van opgeslagen en/of actuele camerabeelden kan alleen gegeven worden door een lid van het managementteam.

Beheer systeem
Systeembeheerders zijn alleen gerechtigd benodigde software te installeren en te controleren op het functioneren van het systeem.

Informatie aan ouders

- Ouders van een leerling die een incident meldt dat het bekijken van camerabeelden noodzakelijk maakt, worden hiervan door de schoolleiding op de hoogte gesteld.
- Indien een leerling – in het belang van het oplossen van een incident – wordt verzocht camerabeelden te bekijken, worden ouders hiervan op de hoogte gesteld. Ouders kunnen het bekijken van de beelden desgewenst bijwonen.
- Ouders van een leerling die na het bekijken van de camerabeelden als “dader” wordt geïdentificeerd, worden hiervan door de schoolleiding op de hoogte gesteld en hebben het recht de beelden binnen de bewaartermijn uit dit protocol te bekijken.
- Camerabeelden die een incident registreren, dat aangifte bij de politie noodzakelijk maakt, kunnen desgevraagd door de politie worden bekeken. Betrokken leerlingen en ouders worden hierover geïnformeerd.

H. Model Protocol ICT en social media voor leerlingen

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 om informatie te zoeken over een onderwerp of werkstuk voor school.
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 linkjes 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 de Whats app. Als ik nare berichten ontvang van iemand, dan vertel ik dit op school of thuis.
12. Als ik iemand niet begrijp via de Whats app 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

De ICT-apparatuur op school (laptop, tablet, 3d-printer, digibord, scanner, etc.) is niet goedkoop, daarom dien je hier voorzichtig mee 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.

D. Schermtijd

17. Ik ben me bewust van de wereld buiten de online wereld en ik houd de tijd in de gaten als ik achter de computer/laptop of tablet zit.

I. Verwerkersovereenkomsten

Leveranciers waarvoor een verwerkersovereenkomst is afgesloten:

☐Actacom
☐Aerobe / RedOrBlue B.V.
☐Aimfor
☐Alles-in-1
☐AMN
☐Ars Scribendi Uitgeverij B.V.
☐Bareka Online Rekentoetsen
☐Basisacademie B.V.
☐BasisOnline
☐Basisschool-apps
☐Bazalt Educatieve Uitgaven
☐BeatsNbits
☐bettermarks NL
☐Blink
☐BLOON
☐Boekgeheim
☐BOLAS
☐Bomberbot
☐Boom uitgevers / Uitgeverij Edu'Actief
☐Boom uitgevers Amsterdam
☐Bordfolio
☐Bosos
☐Brightcenter
☐Briter
☐Brite Wireless Expertise Buro
☐BruutTAAL
☐Bureau Educatief PeuterPlusPlan
☐Bureau ICE
☐CED-Groep
☐Cito
☐ChildPoint
☐Cloudwise B.V.
☐Codename Future
☐Cupella
☐Dageraad
☐DataCare BV
☐Dedact
☐Delta Apps
☐Delubas Educatieve Uitgeverij
☐De Digitale Topschool
☐De Rolf groep
☐De Stoeltjesdans
☐Diataal B.V.
☐DigiDUIF
☐Dotcomschool
☐Driestar Educatief
☐Digikeuzebord
☐Drie-O Automatisering BV
☐Drillster B.V.
☐D. van Dongen advies
☐Educus
☐EduHint B.V.
☐Eisma Edumedia
☐Elerna
☐EURObizz Academy
☐EXOVA
☐Focus Onderwijs B.V.
☐Get There MijnSchool
☐Groot's Onderwijsadvies
☐Gynzy
☐HetSchoolvoorbeeld.nl
☐Heutink ICT
☐Heutink Primair Onderwijs BV
☐Iddink Voortgezet Onderwijs bv
☐iDEALnet
☐IDFocus BV
☐Instruct
☐Intertaal
☐IntraQuest
☐Inzichtelijk Onderwijs
☐IRRUS
☐ISO Groep Automatisering B.V.

☐Isy School B.V.
☐Italko
☐itslearning Nederland
☐Jongbloed Educatief
☐Jimmy Company B.V.
☐Junior Einstein BV
☐Kennisnet
☐KIC
☐Koninklijke Van Gorcum
☐Kwintessens
☐Kwizl
☐LC-Data
☐LearningStone
☐Leerpodium
☐Leeruniek
☐LesLab Coöperatie U.A.
☐LessonUp
☐Liquid Development C.V.
☐Lvscv.nl
☐LWEO
☐Maandtaak (AP-taalproductie)
☐Magnaview
☐Malmberg
☐MaxClass
☐Mijnschoolinfo
☐MIEGROEP Automatisering
☐Muiswerk Educatief
☐Nederlandse Kleurenschool
☐Nils &Paul
☐nnine
☐Noordhoff Uitgevers
☐Oefenweb.nl
☐Onderwijs Transparant BV
☐Onlineklas
☐Onderwijspraktijk Harry Janssens
☐Ontwikkelcentrum
☐OpenEdu
☐OsingadeJong educatieve diensten
☐OVD Educatieve Uitgeverij B.V.
☐ParnasSys
☐Pearson
☐Peppels B.V.
☐Peuter-Kleuterpraktijk Ellen Voogt
☐Presentis B.V.
☐Projects4Learning
☐Prowise B.V.
☐Qompas
☐Quarantainenet
☐Raet
☐Ratho B.V.
☐RealOpen IT
☐ReadSpeaker B.V.
☐Reinders Oisterwijk BV
☐Rovict B.V.
☐RTTI-online B.V.
☐Safe School
☐Scholen met Succes
☐Schoolpoort B.V.
☐Schoolmaster BV
☐Schoolplanner
☐SchouderCom
☐Skool
☐SLB Diensten B.V.
☐Slim
☐Slimleren.nl
☐Smart2Scool
☐SnapIT
☐Snappet
☐SOMtoday b.v.
☐SPEYK
☐Stichting Basispoort
☐Studyflow
☐Summario
☐SWIS Suite, Praktikon
☐Switch IT Solutions bv, Studywise
☐Teachers Channel
☐The Implementation Group (TIG)
☐Thiememeulenhoff
☐Topicus
☐TripleWict

☐Tumult
☐Uitgever Essener
☐Uitgever Zwijsen
☐Uitgeverij Betelgeuze
☐Uitgeverij Deviant b.v.
☐Uitgeverij Malmberg BV
☐Uitgeverij Stoffels BV
☐Unilogic BV
☐VanBuurtICT
☐Van Dijk Educatie bv
☐Van Dijk Educatie, Digitaal Leren
☐Van Tricht uitgeverij
☐Veilig Verkeer Nederland
☐Visiria Uitgeversmaatschappij
☐VO-digitaal
☐VO-content
☐Volution, DataByte BV
☐VSA Vogels Software en Advies
☐VWC
☐Vitasys B.V.
☐Web2work B.V.
☐WIS Services BV
☐WizeNoze B.V.
☐Woordhelder
☐Yubu B.V.
☐Zermelo Software B.V.
☐ZuluBook
☐ZuluDesk
☐Zwijssen
☐…
☐…
☐…

J. Checklist beveiliging ICT

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 Fluvium vindt versleuteld plaats.

Netwerkcomponenten

- De netwerkcomponenten binnen de scholen van Fluvium hebben enkel tot doel dat er gebruik kan worden gemaakt van de digitale omgeving via 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.

Colofon

Auteurs: Privacy op School, Bodegraven 2019