SAMENWERKINGSVERBAND
PASSEND ONDERWIJS VO 22.03
HOOGEVEEN MEPPEL STEENWIJK

Informatiebeveiligings- en privacybeleid

Samenwerkingsverband VO 22.03

Versie	Status	Datum	Omschrijving
1.0	concept	05-04-2022	IBP + bijlagen

Besproken met DB:

Versie	Status	Datum	Omschrijving
1.0	concept		IBP + bijlagen

Besproken met AB:

Versie	Status	Datum	Omschrijving
1.0	concept		IBP + bijlagen

Ingestemd door OPR:

Versie	Status	Datum	Omschrijving
1.0			IBP + bijlagen

Vastgesteld door:

Versie	Datum	Naam	Functie
1.0		E. van de Waeter	Directeur

SAMENWERKINGSVERBAND
PASSEND ONDERWIJS VO 22.03
HOOGEVEEN MEPPEL STEENWIJK

Inhoudsopgave

1 Het belang van informatiebeveiliging en privacy

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

2 Toelichting informatiebeveiliging en privacy

2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:

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

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

2.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

2.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen SWV VO 22.03 te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan SWV VO 22.03 persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en betrokkenen.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. leerlingen en hun ouders/verzorgers) wordt gerespecteerd en SWV VO 22.03 voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen SWV VO 22.03 geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers, externe relaties (inhuur / outsourcing) en overige betrokkenen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het netwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen SWV VO 22.03 waaronder in ieder geval medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers, externe relaties (inhuur / outsourcing) en overige betrokkenen waarvan SWV VO 22.03 persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van SWV VO 22.03. Hieronder valt tevens de gecontroleerde informatie, die door de organisatie zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)
- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van SWV VO 22.03 evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- IBP-beleid heeft binnen SWV VO 22.03 raakvlakken met:
  - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
  - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
  - *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
  - *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

4 Beleid – Hoe doen we dat?

SWV VO 22.03 hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het algemeen bestuur van SWV VO 22.03 neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. De directeur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is de directeur de verwerkingsverantwoordelijke.

2. SWV VO 22.03 voldoet aan alle relevante wet- en regelgeving.

3. Bij SWV VO 22.03 is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van SWV VO 22.03 om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.

4. SWV VO 22.03 zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.

5. SWV VO 22.03 legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. SWV VO 22.03 voldoet hiermee aan de documentatieplicht.

6. Binnen SWV VO 22.03 is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.

7. SWV VO 22.03 is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de organisatie informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. SWV VO 22.03 classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

9. SWV VO 22.03 sluit met alle leveranciers van digitale middelen verwerkersovereenkomsten af als zij, in opdracht van de organisatie, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.

10. SWV VO 22.03 verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. SWV VO 22.03 heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij SWV VO 22.03 een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. SWV VO 22.03 kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. SWV VO 22.03 neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het passend onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.
    Daar waar de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt SWV VO 22.03 aanvullende afspraken vast over de technische maatregelen.

14. SWV VO 22.03 zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

5 Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

5.1 Relevante wet- en regelgeving

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

- Wet op het voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht
- Artikel 17a van de wet op het Voortgezet Onderwijs (WVO)

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

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

5.2 Basisregels bij het omgaan met persoonsgegevens

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

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven

en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.

3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**: het samenwerkingsverband legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

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

5.3 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

5.4 Voorlichting en bewustzijn

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

5.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.6 Incidenten en datalekken

Alle betrokkenen, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij E. van de Waeter, evandewaeter@vo2203.nl.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7 Planning en controle

Dit IBP-beleid wordt minimaal elk jaar getoetst en, indien nodig, bijgesteld door de directeur. Hierbij wordt rekening gehouden met:

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

Daarnaast kent SWV VO 22.03 een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

5.8 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de directeur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan SWV VO 22.03 de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.9 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

Organisatie - Wie doet wat?

Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij SWV VO 22.03.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Directeur	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen

Sturend (tactisch)	Beleidsmedewerker (o.a. voor IBP)	• Inhoudelijk verantwoordelijk voor IBP
		• IBP-planning en controle
		• Adviseert directie over IBP
		• Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse
		  • Hanteren IBP normen en wijze van toetsen
		  • Evalueren IBP-beleid en maatregelen
		  • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze
		  • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen
			Processen, richtlijnen en procedures IBP, waaronder:
			• activiteitenkalender
			• Protocol beveiligingsincidenten en datalekken
			• Verwerkersovereenkomsten regelen
			• Brief toestemming gebruik beeldmateriaal
			• Opstellen informatie documentatie richting leerlingen, ouders / verzorgers
			• Security awareness activiteiten
			• Sociale media reglement
			• Gedragscode ict en internetgebruik
			• Gedragscode medewerkers en leerlingen

	Functionaris voor Gegevensbescherming	• Toezicht op naleving privacy wetgeving • Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.:	• **Classificatie / risicoanalyse** in samenwerking met verantwoordelijke IBP	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister

	ICT, HRM / P&O, facilitair, onderwijs, financiën, inkoop en administratie	• Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door directie • Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
Uitvoerend (operationeel)	Systeembeheerder Medewerker Directeur	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken

De verdere uitwerking van de rollen en taken staan beschreven in bijlage 2.

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Documenten:	Aandachtspunten:
Procedure voor verwijderen van gegevens	bewaartermijnen
Procedure rondom uitwisselen gegevens	Passend onderwijs, leerling dossiers, leerplicht etc
Communicatie rechten betrokkenen	Communicatie richting betrokkenen
Procesbeschrijving rechten betrokkenen	Proces rondom aanvragen van betrokkenen
Privacyreglement	
Autorisatiematrix	Wie mogen gegevens inzien, bewerken enz
Afspraken gebruik sociale media	
Procedure rondom training medewerkers	Bewustzijn creëren
Wachtwoordbeleid	
Responsible disclosure	Procedure voor het melden van vermoedelijke beveiligingsincidenten
Gedragscode ict en internetgebruik	Verantwoord gebruik bedrijfsmiddelen

Verplicht vanuit de AVG:

Procesbeschrijving melden datalekken	
Registratie beveiligingsincidenten	
Dataregister om te voldoen aan de registratieplicht	
Verwerkersovereenkomsten	Privacy bijlage beschikbaar stellen
Procedure gegevensbeschermingseffectbeoordeling	DPIA
Risicoanalyse	
Functionaris voor Gegevensbescherming	Communicatie hierover richting medewerkers

Bijlage 2: Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij SWV VO 22.03 voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen. Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Eindverantwoordelijke
De directeur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd.
De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de beleidsmedewerker.

Sturend

Beleidsmedewerker en directeur
Beleidsmedewerker en directeur zijn rollen op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De beleidsmedewerker en directeur moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen SWV VO 22.03
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen SWV VO 22.03 coördineren

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG), binnen SWV VO 22.03 houdt toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het bestuur). De FG heeft regelmatig overleg met manager IBP. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Uitvoerend

Systeembeheerder
De systeembeheerder vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.
Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De functioneel beheerder wordt vanuit de directeur voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

.

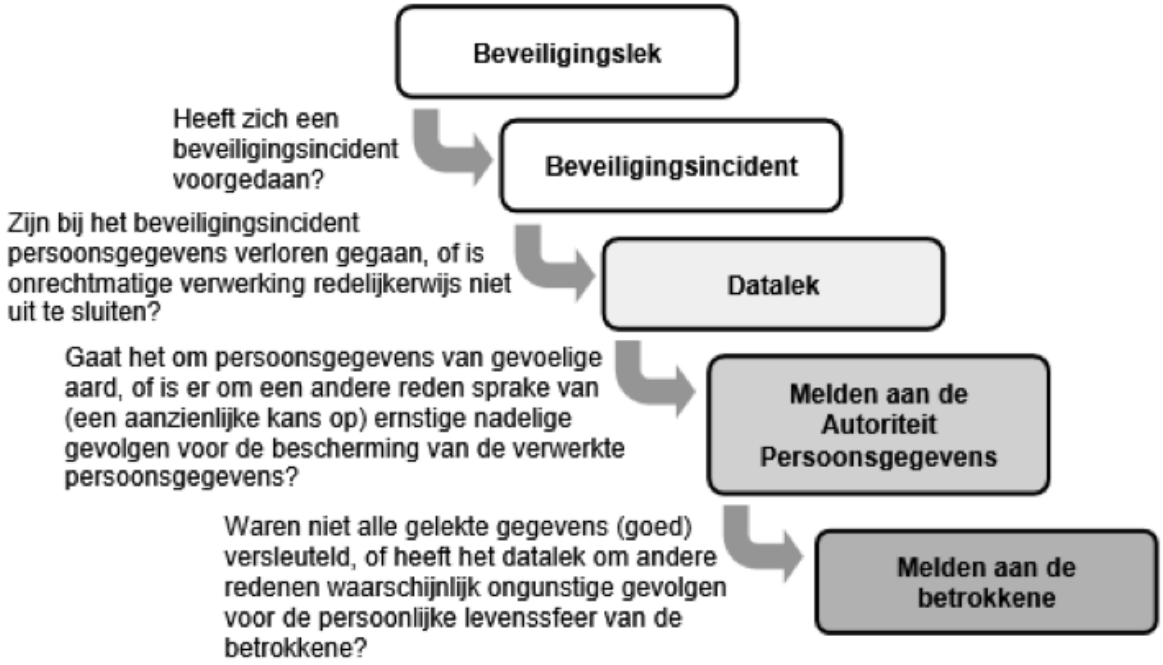
Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. de zorgvuldigheidsverklaring en de protocol gebruik bedrijfsmiddelen. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.
Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de OPR)

Contactgegevens

Eindverantwoordelijke	E. van de Waeter (directeur)	e.vandewaeter@vo2203.nl
FG	A. Engels (Akorda)	info@akorda.nl
Beleidsmedewerker	M. Sinnema	msinnema@vo2203.nl
ICT	Bloemert ICT	

Bijlage 3: Datalekkenprotocol

Bij de beslissing of een gebeurtenis die zich heeft voorgedaan moet worden gemeld aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moeten een aantal afwegingen gemaakt worden. Het onderstaande schema geeft deze afwegingen weer.



Datalek
Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident kan gedacht worden aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker, vermissing van een papieren dossier of dossierstukken.

Niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs uitgesloten kunnen worden.

Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. Er hoeft dan geen melding gedaan te worden aan de Autoriteit Persoonsgegevens.

Melden aan de autoriteit Persoonsgegevens
SWV VO 2203 is in een aantal gevallen verplicht om een datalek te melden aan de Autoriteit Persoonsgegevens. Volgens de wet moet een melding aan de Autoriteit Persoonsgegevens gedaan worden als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk.

Bij persoonsgegevens van gevoelige aard moet gedacht worden aan:

- Bijzondere persoonsgegevens
  Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke

persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

- Gegevens over de financiële of economische situatie van de betrokkene
  - Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
  - (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- Gebruikersnamen, wachtwoorden en andere inloggegevens
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude
  Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Melden aan betrokkene
In een aantal gevallen waarin een datalek gemeld wordt aan de Autoriteit Persoonsgegevens moet deze ook worden gemeld aan de betrokkene. De wet geeft aan dat een melding gedaan moet worden aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Daarbij kan bijvoorbeeld gedacht worden aan onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits-)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt dan moet het datalek ook gemeld worden aan de betrokkene.

De melding stelt de betrokkene in staat om alert te zijn op de mogelijke gevolgen van het datalek en om zich daar waar mogelijk tegen te wapenen door, bijvoorbeeld, een gelekt wachtwoord te vervangen. Indien er gemeld moet worden dan zullen de betrokkenen onverwijld op de hoogte gesteld worden zodat de betrokkene naar aanleiding van de melding in staat wordt gesteld maatregelen te nemen om zich te beschermen tegen de gevolgen van het datalek.

Afspraken met de verwerker
SWV VO 22.03 heeft als verantwoordelijke een zorgplicht t.a.v. een eventueel opgetreden datalek bij een verwerker. Zij zorgt er in dit geval voor dat zij haar wettelijke verplichting kan nakomen en legt met de verwerker vast dat zij tijdig en adequaat geïnformeerd wordt over datalekken waarvan hij/zij kennis krijgt. Zij wil in alle gevallen geïnformeerd worden t.a.v. datalekken bij verwerkende partijen.

SWV VO 22.03 maakt de volgende afspraken met de verwerker:

1. De verwerker informeert SWV VO 22.03 onverwijld over alle relevante incidenten.
2. De verwerker meldt zelf datalekken aan de Autoriteit persoonsgegevens en verzendt een afschrift van deze melding naar de Functionaris gegevensbescherming.
3. De verwerker houdt SWV VO 22.03 op de hoogte van nieuwe ontwikkelingen rond het gemelde datalek incident en van de maatregelen die getroffen worden aan de kant van de bewerker om herhaling van het incident te voorkomen.

De gemaakte afspraken worden vastgelegd in de verwerkersovereenkomsten. Voor veel verwerkers geldt dat zij aangesloten zijn bij Privacy Convenant Onderwijs en daarmee het Privacy Protocol Onderwijs en de Verwerkersovereenkomst hanteren.

Meldingsprotocol
Alle medewerkers van SWV VO 22.03 zijn verplicht onverwijld een melding te doen van een geconstateerd datalek. Voorbeelden van datalekken zijn: een gestolen laptop, tablet, telefoon, of een inbraak in een databestand of applicatie, ontvreemding toegangscodes van applicaties en dergelijke.

De melding dient te gebeuren bij de directeur van SWV VO 22.03. De directeur doet de melding bij de Functionaris Gegevensbescherming en neemt maatregelen ter voorkoming van verdere schade. Op basis van de melding wordt aan de hand van de leidraad van de Autoriteiten Persoonsgegevens beslist of er gemeld moet worden bij de Autoriteit Persoonsgegevens en/of de betrokkene(n).

Functionaris Gegevensbescherming

Organisatie: Akorda Onderwijsdienstverlening
Vrouwenlaan 125
8017 HR Zwolle

Naam: Mr. A. Engels
Email: info@akorda.nl
Telefoon: 038 465 9814

Vastleggen meldingen

Meldingen van datalekken worden vastgelegd op een registratieformulier. Bij de melding wordt vastgelegd wat de aard is van de gegevens die zijn gelekt, onder welke omstandigheden het lek is ontstaan, door wie de melding is gedaan, of er een melding bij de Autoriteit Persoonsgegevens is gedaan, of de betrokkene (degene wiens gegevens zijn gelekt) is geïnformeerd, welke maatregelen er zijn genomen ter bescherming van de bij het datalek betrokken personen, de status van afhandeling en de genomen maatregelen ter voorkoming van de lekkage in de toekomst. Op de volgende pagina wordt een voorbeeld van het registratie weergegeven. Het daadwerkelijke formulier kunt u vinden op: www.swvvo2203.nl

SAMENWERKINGSVERBAND PASSEND ONDERWIJS VO 22.03

HOOGEVEEN MEPPEL STEENWIJK

Registratieformulier beveiligingsincident/datalek

Datum / periode van beveiligingsincident

Naam melder / ontdekker

Functie melder / ontdekker

E-mailadres melder / ontdekker

Plaats van incident

- ○ School
- ○ Stichting
- ○ Elders namelijk:

Gevolg / schade

- ○ Ja
- ○ Nee (naar verwachting)
- ○ Weet niet

Gevolgen voor privacy

- ○ Ja
- ○ Nee
- ◉ Weet niet

Toedracht van het incident

Korte omschrijving van het incident

Datalek

- ○ Ja
- ○ Nee

Type gegevens in kwestie

Welke acties zijn ondernomen

Onderstaande gegevens dient Meldpunt in te vullen.

Melden bij Autoriteit Persoonsgegevens

- ◉ Ja
- ○ Nee

Nummer incident

Zijn betrokken geïnformeerd?

- ○ Ja
- ◉ Nee

Aanvullende opmerkingen

Bijlage 4: privacyreglement

Inleiding

Samenwerkingsverbanden passend onderwijs hebben persoonsgegevens van leerlingen nodig om hun taken goed te kunnen uitoefenen. De wet passend onderwijs (artikel 18a lid 13 Wpo, artikel 17a Wvo) heeft dit geregeld door onder meer te bepalen dat het samenwerkingsverband bevoegd is om zonder toestemming van de betrokken leerling of diens wettelijk vertegenwoordiger persoonsgegevens mag verwerken die nodig zijn voor het vervullen van de wettelijke taak van het samenwerkingsverband.

Deze gegevens zal het samenwerkingsverband ontvangen van de school die een leerling aanmeldt in het kader van een verzoek om extra ondersteuning (voor het toekennen van een ondersteuningsarrangement, voor advies inzake extra ondersteuning of voor het beoordelen van de toelaatbaarheid van een leerling tot het (voortgezet) speciaal onderwijs). Dit kan een ingeschreven dan wel een aangemelde leerling zijn.

Om deze taken te kunnen uitvoeren, zal het samenwerkingsverband persoonsgegevens verwerken. Hierbij geldt vanaf 25 mei 2018 de Algemene verordening gegevensbescherming (AVG); dit is de Europese privacy-regelgeving die vanaf 25 mei 2018 ook in Nederland van toepassing is en de Wet bescherming persoonsgegevens opvolgt.

Samenwerkingsverbanden verwerken voor een deel ‘gewone’ persoonsgegevens, dat wil zeggen gegevens die niet zijn aan te merken als bijzondere persoonsgegevens als bedoeld in de AVG. Te denken valt aan naam, adres en woonplaats en overige contactgegevens van de leerling. Daarnaast gaat het bij de gegevensverwerkingen in het kader van passend onderwijs om zogenaamde ‘bijzondere’ persoonsgegevens, bijvoorbeeld over gezondheid als bedoeld in de AVG.[1]

Grondslag voor gegevensverwerking
Om *persoonsgegevens* te mogen verwerken stelt de AVG de eis dat de verwerking gebaseerd dient te zijn op een grondslag als genoemd in artikel 6 AVG.
Die grondslag is voor samenwerkingsverbanden primair gelegen in de wettelijke verplichting om taken uit te voeren ten behoeve van de aangesloten schoolbesturen. Het gaat wettelijk om 3 taken in dit verband:

1. Het toelaatbaar verklaren van leerlingen tot (voortgezet) speciaal onderwijs, het speciaal basisonderwijs en het praktijkonderwijs en het geven aan aanwijzingen voor Leerweg ondersteunend onderwijs (LWOO);
2. Het geven van adviezen aan de aangesloten scholen over de ondersteuningsbehoefte van leerlingen;
3. Het toekenning van middelen voor extra ondersteuning en -voorzieningen aan scholen, ten behoeve van de ondersteuning van leerlingen.

De wetgever geeft voor het vervullen van deze taken in de wet passend onderwijs een wettelijke grondslag aan samenwerkingsverbanden om hiertoe persoonsgegevens te bewerken. Voor bovenstaande drie taken mogen samenwerkingsverbanden en aangesloten scholen/schoolbesturen zonder toestemming van ouders persoonsgegevens uitwisselen. Ouders dienen wel op de hoogte te zijn van het feit dat dit gebeurt en moeten in staat worden gesteld om gegevens in te zien of te corrigeren. Aan derden, behalve de bevoegde gezagsorganen van de betrokken scholen, mogen deze gegevens *niet* worden verstrekt.

Algemeen belang als grondslag
Naast deze wettelijke grondslag formuleert de AVG ook de grondslag dat verwerking rechtmatig is ‘om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen’. Ook hiervan kan sprake zijn bij passend onderwijs. Uitwisseling van persoonsgegevens tussen een samenwerkingsverband en een

[1] Het begrip gezondheid dient ruim te worden opgevat en omvat alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen. Ook gegevens over handicap en sociaal-emotionele problematiek vallen onder het begrip gezondheid.

school of een derde partij (bijvoorbeeld een jeugdhulpinstelling) kan nodig zijn om voor de leerling een ononderbroken ontwikkelingsproces te realiseren, om thuiszitten tegen te gaan, etc.
De AVG formuleert ook de grondslag 'nodig in het algemeen belang' of 'nodig voor een gerechtvaardigd belang'. Samenwerkingsverbanden zullen in het kader van het tegengaan van thuiszitters ook gegevens verwerken op basis van overleg met bijvoorbeeld gemeenten en leerplicht. Dit zal nodig zijn vanwege het algemeen belang dat hiermee is gediend en heeft ook een wettelijke basis omdat samenwerkingsverbanden wettelijk verplicht zijn om de Onderwijsinspectie te informeren over aantallen en duur van thuiszitters.

Samenwerkingsverbanden die persoonsgegevens verwerken voor andere taken dan de drie taken die hierboven zijn genoemd, dienen zich dus te kunnen beroepen op een van de volgende grondslagen van de AVG: 'bescherming vitaal belang betrokkene', 'nodig in het algemeen belang' of 'nodig voor een gerechtvaardigd belang'. Bij het laatste belang moet het samenwerkingsverband kunnen aantonen dat het belang van het samenwerkingsverband zwaarder weegt dan het belang van betrokkene om bescherming van persoonsgegevens.

Verwerkingsverantwoordelijke en verwerker
Het samenwerkingsverband is conform de AVG een 'verwerkingsverantwoordelijke' en geen 'verwerker'. Een verwerker is een instantie die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Een administratiekantoor die de personeelsgegevens van het samenwerkingsverband verwerkt, is zo'n verwerker. Hiermee dient het samenwerkingsverband een verwerkersovereenkomst te sluiten.

Een verwerkingsverantwoordelijke is het orgaan die zelf met een bepaald doel en bepaalde middelen persoonsgegevens bewerkt. Het samenwerkingsverband is een orgaan met een wettelijke opdracht waartoe het nodig is om persoonsgegevens te bewerken en daarmee een 'verwerkingsverantwoordelijke'.

Principes en verantwoordingsplicht
De AVG formuleert een aantal belangrijke principes voor gegevensverwerking:

- Het gebeurt op een wijze die rechtmatig, behoorlijk en transparant is;
- Het gebeurt alleen voor een uitdrukkelijk omschreven en gerechtvaardigd doel (doelbinding):
- Het beperkt zich tot wat noodzakelijk is voor het doel waarvoor het wordt verwerkt (minimale gegevensverwerking);
- Het gaat om juiste en geactualiseerde gegevens met redelijke maatregelen om waar nodig te rectificeren of te wissen (juistheid).

Het onderstaande reglement is gebaseerd op deze principes. De AVG vermeldt ten aanzien van deze principes dat de verwerkingsverantwoordelijke ten allen tijde in staat is om aan te tonen dat het zich hieraan houdt (verantwoordingsplicht). Om die reden is het wenselijk en noodzakelijk dat elk samenwerkingsverband niet alleen een register verwerkingsactiviteiten heeft (waarin alle verwerkingen zijn vastgelegd, wettelijk verplicht) maar ook systematisch beleid heeft ontwikkeld (bijvoorbeeld in een privacy-handboek) waarin is vastgelegd wat de interne procedures zijn ten aanzien van gegevensbescherming, wie waar bij mag, en waaruit blijkt dat sprake is van bijvoorbeeld minimale gegevensverwerking (bijvoorbeeld uit de gemaakte afspraken met de toeleverende scholen welke gegevens wel of niet worden gevraagd en waarom die gegevens noodzakelijk zijn.

Functionaris Gegevensbescherming
De AVG introduceert de Functionaris Gegevensbescherming. Ook samenwerkingsverbanden dienen zo'n functionaris te hebben. Het is niet noodzakelijk dat die persoon in dienst is, het mag ook een functionaris zijn die wordt 'ingehuurd' en op basis van een dienstverleningsovereenkomst werkzaam is. Het is belangrijk dat de functionaris onafhankelijk zijn werkzaamheden kan verrichten en vrij is om adviezen te geven aan het samenwerkingsverband over de inrichting van de gegevensverwerking. Op de website van de Autoriteit Gegevensbescherming is meer te vinden over de taken van de FG: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/functionaris-voor-de-gegevensbescherming-fg. In het reglement is opgenomen dat het samenwerkingsverband een FG heeft aangewezen.

In onderstaand privacyreglement is een en ander samengebracht. Er worden diverse begrippen gehanteerd. Hierbij is bij ‘verwerkingsverantwoordelijke’ te denken aan het (bestuur van het) samenwerkingsverband, bij ‘verwerker’ aan externen die in opdracht van het samenwerkingsverbanden gegevens bewerken (bijvoorbeeld het administratiekantoor) en bij ‘deskundigen’ aan een orthopedagoog en een tweede deskundige als een kinder- of jeugdpsycholoog, een pedagoog, een maatschappelijk werker, een arts of een kinderpsychiater. Personeel dat werkzaam is voor het samenwerkingsverband op basis van dienstverband of detachering en persoonsgegevens verwerkt is geen ‘verwerker’ (is niet extern) maar valt onder de ‘verwerkingsverantwoordelijke’.
Bij wettelijk vertegenwoordiger denkt men bijvoorbeeld aan degene die het ouderlijk gezag of de voogdij uitoefent.
Ten slotte, overal waar ‘hem’ of ‘hij’ is vermeld, kan ook ‘haar’ of ‘zij’ worden gelezen.

Privacyreglement Samenwerkingsverband Passend Onderwijs Voortgezet Onderwijs 22.03

Artikel 1 Begripsbepalingen
In dit reglement wordt verstaan onder:

a. **AVG**: Algemene Verordening Gegevensbescherming van 27 april 2016 van de Europese Unie;
b. **Autoriteit Persoonsgegevens (AP)**: de toezichthouder op de naleving van de AVG, voorheen het College Bescherming Persoonsgegevens;
c. **bestand**: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;
d. **persoonsgegeven**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon;
e. **verwerking van persoonsgegevens**: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
f. **verwerkingsverantwoordelijke**: het samenwerkingsverband, dat wil zeggen de rechtspersoon als bedoeld in artikel 18a Wpo respectievelijk artikel 17a Wvo, dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
g. **verwerker**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van het samenwerkingsverband persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
h. **betrokkene**: degene op wie een persoonsgegeven betrekking heeft (waaronder personeel en leerlingen;
i. **derde**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;
j. **toestemming van de betrokkene**: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;
k. **verzamelen van persoonsgegevens**: het verkrijgen van persoonsgegevens;
l. **leerling**: een leerling die extra ondersteuning behoeft, of waarvan dit wordt vermoed, bij het volgen van onderwijs op een school voor primair -, speciaal - of voortgezet (speciaal) onderwijs zoals bedoeld in de Wpo, Wvo en Wec en die is aangemeld dan wel ingeschreven bij een school gelegen in de regio of woont in de regio en is aangemeld of ingeschreven bij een school buiten de regio;
m. **scholen (school)**: alle vestigingen van basisscholen, van speciale scholen voor basisonderwijs, van scholen voor speciaal onderwijs, van scholen voor voortgezet onderwijs, van scholen voor voortgezet speciaal onderwijs en van scholen voor speciaal en voortgezet speciaal onderwijs, voor zover daaraan speciaal onderwijs dan wel voortgezet speciaal onderwijs wordt verzorgd, behorend tot cluster 3 en 4 bedoeld in de Wet op de expertisecentra en gevestigd in de regio;
n. **regio**: het bij ministeriële regeling aan het samenwerkingsverband aangewezen aaneengesloten gebied waarbinnen het samenwerkingsverband haar doel verwezenlijkt;
o. **Wpo**: Wet op het primair onderwijs;
p. **Wvo**: Wet op het voortgezet onderwijs;
q. **Wec**: Wet op de expertisecentra;

Artikel 2 Reikwijdte en doelstelling van het reglement

1. Dit reglement is van toepassing op alle persoonsgegevens van een betrokkene die door of namens het bestuur van het Samenwerkingsverband VO 2203 worden verwerkt.

2. Dit reglement heeft tot doel:
   a. vast te stellen van welke personen het samenwerkingsverband persoonsgegevens verwerkt;
   b. de persoonlijke levenssfeer van een betrokkene van wie persoonsgegevens worden verwerkt te beschermen tegen misbruik van die gegevens en tegen het verwerken van onnodige en onjuiste persoonsgegevens evenals tegen de verwerking op onjuiste of niet nauwkeurige wijze;
   c. te voorkomen dat persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze verzameld zijn;
   d. de rechten van een betrokkene te waarborgen.

Artikel 3 Categorieën van de personen in de verwerking (betrokkene(n))
Persoonsgegevens worden verwerkt van de bij het samenwerkingsverband aangemelde leerling.

Artikel 4 Doelstellingen van verwerking persoonsgegevens en toestemming
1. De verwerking van persoonsgegevens geschiedt ten behoeve van de realisatie van een samenhangend geheel van ondersteuningsvoorzieningen binnen en tussen de scholen in de regio van het samenwerkingsverband opdat leerlingen die extra ondersteuning behoeven een zo passend mogelijke plaats in het onderwijs krijgen.

2. De persoonsgegevens kunnen verder geanonimiseerd en niet meer herleidbaar tot een persoon gebruikt worden voor door het samenwerkingsverband georganiseerde beschrijvende, evaluatieve en onderzoeksmatige doeleinden inzake de geconstateerde ondersteuningsvraag van scholen en het aanbod van het samenwerkingsverband alsmede ten behoeve van beleidsvoering ter verbetering van de kwaliteit noodzakelijk ter uitvoering van de doelstellingen. Hierbij worden geen gegevens verwerkt die betrekking hebben op naam, adres, postcode of gegevens die in combinatie met elkaar herleidbaar zijn tot betrokkene.

3.Het samenwerkingsverband is bevoegd zonder toestemming van de leerling dan wel diens wettelijk vertegenwoordiger algemene en bijzondere persoonsgegevens van de leerling te verwerken, ten behoeve van:
a. het verdelen en toewijzen van ondersteuningsmiddelen en ondersteuningsvoorzieningen aan de scholen,
b. het beoordelen of leerlingen toelaatbaar zijn tot het onderwijs aan een speciale school voor basisonderwijs in het samenwerkingsverband of tot het speciaal onderwijs of tot het voortgezet speciaal onderwijs, op verzoek van het bevoegd gezag van een school waar de leerling is aangemeld of ingeschreven
c. het beoordelen of leerlingen zijn aangewezen op leerwegondersteunend onderwijs, op verzoek van het bevoegd gezag van een school waar de leerling is aangemeld of ingeschreven, en
d. het adviseren over de ondersteuningsbehoefte van een leerling op verzoek van het bevoegd gezag van een school waar de leerling is aangemeld of ingeschreven, waaronder het bieden van orthopedagogische/didactische ondersteuning (OPDC) aan de leerling

Artikel 5 Verwerkingsverantwoordelijke
Het samenwerkingsverband is voor de verwerking verantwoordelijk voor de verwerking overeenkomstig de bepalingen van de Wpo, de Wvo en de daarop gebaseerde algemene maatregelen van bestuur en dit reglement. De verwerkingsverantwoordelijke treft daartoe de nodige voorzieningen, waaronder in elk geval zodanige opslag van persoonsgegevens dat deze niet voor onbevoegden toegankelijk zijn.

Artikel 6 Opname van gegevens en informatieplicht
1. Over de personen, zoals bedoeld in artikel 3 , kunnen uitsluitend gegevens worden opgenomen voor zover verstrekt door de betrokkene, diens wettelijk vertegenwoordiger, de school, deskundigen of deskundige instanties. Persoonsgegevens verkregen op andere dan de in de eerste volzin bedoelde wijze kunnen slechts worden opgenomen indien de betrokkene daar toestemming[2] voor geeft en voor zover de gegevens zich

[2] Indien de betrokkene minderjarig is en de leeftijd van zestien jaren nog niet heeft bereikt, of onder curatele is gesteld dan wel ten behoeve van de betrokkene een mentorschap is ingesteld, is in de plaats van de toestemming van de betrokkene die van zijn wettelijk

daarvoor lenen en voor zover dat noodzakelijk is voor de doelstelling van de verwerking.
2. Wanneer persoonsgegevens worden verwerkt doet de verwerkingsverantwoordelijke daarvan mededeling aan de betrokkene dan wel diens wettelijk vertegenwoordiger en deelt hij de doeleinden van de verwerking waarvoor de gegevens zijn bestemd aan de betrokkene dan wel diens wettelijk vertegenwoordiger mee, tenzij de betrokkene dan wel diens wettelijk vertegenwoordiger daarvan reeds op de hoogte is.
3. In alle gevallen worden in de verwerking uitsluitend persoonsgegevens opgenomen die noodzakelijk zijn ter verwezenlijking van het doel waarvoor zij worden verzameld. De verwerkingsverantwoordelijke treft de nodige maatregelen opdat de verzameling en verwerking van de persoonsgegevens op juiste en nauwkeurige wijze geschiedt.

Artikel 7 Soorten van gegevens
Met betrekking tot de in artikel 3 genoemde personen worden geen andere persoonsgegevens verwerkt dan:

b. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de betrokkene;
c. nationaliteit;
d. gegevens als bedoeld onder a, van de wettelijk vertegenwoordiger of verzorger van de leerling;
e. gegevens betreffende de gezondheid of het welzijn van de leerling voor zover die noodzakelijk zijn voor de ondersteuning;
f. gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor de ondersteuning;
g. gegevens betreffende de aard en het verloop van het onderwijs en ondersteuning, alsmede de behaalde studieresultaten;
h. gegevens met het oog op de organisatie van de ondersteuning (waaronder OPDC) en het verstrekken of ter beschikking stellen van ondersteuningsmiddelen of voorzieningen;
i. schoolgegevens (waaronder naam school, naam zorgcoördinator/mentor/ intern begeleider, klas/groep waarin de leerling zit, tijdstip van inschrijving bij deze school, naam van de indiener van de aanmelding bij het samenwerkingsverband, schoolloopbaan en rapportage vanuit primair en voortgezet onderwijs);
j. aanleiding voor de aanmelding bij het samenwerkingsverband, relevante screenings- en onderzoeksgegevens en omschrijving van de problematiek die aan de orde is;
k. activiteiten die door de school zijn ondernomen rond de betreffende leerling, alsmede de resultaten hiervan;
l. bestaande of (relevante) afgesloten hulpverleningscontacten en de namen van contactpersonen;
m. relevante persoonsgegevens die door externe partijen worden verstrekt met betrekking tot de aangemelde problematiek van de betreffende leerling;
n. het opgestelde onderwijskundige rapport en/of het ontwikkelingsperspectief van de aangemelde leerling;
o. gegevens over voortgang, de evaluatie en de afsluiting van de ingestelde ondersteuning;
p. andere dan de onder a tot en met o bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een wettelijke regeling.

Artikel 8 Toegang tot persoonsgegevens
1. De verwerkingsverantwoordelijke voor de verwerking verleent slechts toegang tot de in de verwerking opgenomen persoonsgegevens aan:

vertegenwoordiger vereist. Een toestemming kan door de betrokkene of zijn wettelijk vertegenwoordiger te allen tijde worden ingetrokken.

a. de verwerker en de persoon die onder rechtstreeks gezag van de verwerkingsverantwoordelijke, of de verwerker gemachtigd is om persoonsgegevens te verwerken alsmede de deskundigen, bedoeld in artikel 18a Wpo lid 11 en in artikel 17a Wvo lid 12[3].
b. degenen aan wie krachtens wettelijk voorschrift toegang dient te worden verleend, echter niet dan deugdelijke legitimatie.

2. Degenen genoemd in lid 1 van dit artikel worden door het samenwerkingsverband geregistreerd in een daartoe door de verwerkingsverantwoordelijke ingericht bestand dat als bijlage 1 bij dit reglement wordt gevoegd.

Artikel 9 Verstrekking van gegevens

1. De verwerkingsverantwoordelijke voor de verwerking verstrekt persoonsgegevens uit de verwerking slechts aan anderen dan de in artikel 8 genoemde personen uitsluitend en voor zover:
    a. de verwerkingsverantwoordelijke daartoe op grond van enige wettelijke bepaling verplicht is;
    b. de betrokkene op wie de te verstrekken gegevens betrekking heeft of diens wettelijk vertegenwoordiger daarin heeft toegestemd.
2. De verwerkingsverantwoordelijke verstrekt de gegevens, bedoeld in artikel 4 lid 3 van dit reglement, niet aan derden, met uitzondering van het bevoegd gezag van de school waar de desbetreffende leerling is aangemeld of ingeschreven.
3. Van de verstrekking van gegevens als bedoeld in dit artikel houdt de verwerkingsverantwoordelijke deugdelijk aantekening.

Artikel 10 Beveiliging en geheimhouding

1. De verwerkingsverantwoordelijke draagt zorg voor passende technische en organisatorische maatregelen ter voorkoming van verlies of onrechtmatige verwerking van persoonsgegevens. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

2. Indien sprake is van elektronische verwerking van persoonsgegevens zal het samenwerkingsverband via een coderings- en wachtwoordbeveiliging de verschillende personen, als bedoeld in artikel 8, toegang geven tot bepaalde gedeelten van de persoonsgegevens of tot alle persoonsgegevens al naar gelang hun werkzaamheden dit vereisen.

3. Een ieder die betrokken is bij de uitvoering van dit reglement en daarbij de beschikking krijgt over persoonsgegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift ter zake van de persoonsgegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan. Dit geldt niet indien enig wettelijk voorschrift hem tot bekendmaking verplicht of uit zijn taak bij de uitvoering van dit reglement de noodzaak tot bekendmaking voortvloeit.

Artikel 11 Rechten betrokkene(n): inzage, correctie, verwijdering

1. Elke betrokkene dan wel diens wettelijk vertegenwoordiger heeft het recht op inzage. Het recht op inzage omvat het recht op het verkrijgen van kopieën van de persoonsgegevens. Aan een verzoek om inzage kunnen administratieve kosten worden verbonden.
2. Indien de verwerkingsverantwoordelijke twijfelt aan de identiteit van de verzoeker, vraagt hij zo spoedig mogelijk aan de verzoeker schriftelijk nadere gegevens inzake zijn identiteit te verstrekken of een geldig

[3] Dit zijn de deskundigen die advies geven over de toelaatbaarheid van leerlingen tot het SBO of (V)SO zoals een orthopedagoog en door een tweede deskundige als een kinder- of jeugdpsycholoog, een pedagoog, een maatschappelijk werker, een arts of een kinderpsychiater (zie de concept AMvB zoals deze voor consultatie gepubliceerd is op 28 februari 2013).

identiteitsbewijs te overleggen. Door dit verzoek wordt de termijn opgeschort tot het tijdstip dat het gevraagde bewijs is geleverd.
3. Een verzoek om inzage dient te worden gedaan aan de verwerkingsverantwoordelijke, die binnen vier weken na ontvangst van dit verzoek hierop schriftelijk reageert middels het tenminste ter beschikking stellen van een volledig overzicht van de hem betreffende persoonsgegevens in een begrijpelijk vorm en een omschrijving van de doeleinden van de verwerking met inlichtingen over de herkomst daarvan.
4. Indien de betrokkene dan wel diens wettelijke vertegenwoordiger de verwerkingsverantwoordelijke verzoekt tot verbetering, aanvulling, verwijdering of afscherming (correctie) omdat bepaalde opgenomen gegevens onjuist c.q. onvolledig zouden zijn, dan wel voor de doelstelling van de verwerking onvolledig of niet ter zake doen, dan wel strijdig zijn met dit reglement of een wettelijk voorschrift, neemt de verwerkingsverantwoordelijke binnen vier weken nadat betrokkene dan wel diens wettelijk vertegenwoordiger dit verzoek heeft ingediend, hierover een beslissing.
5. De verwerkingsverantwoordelijke bericht de verzoeker schriftelijk of en in hoeverre hij aan het verzoek voldoet. Een weigering is met redenen omkleed.
6. De verwerkingsverantwoordelijke draagt zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.
7. De verwerkingsverantwoordelijke is verplicht om aan derden aan wie de gegevens daaraan voorafgaand zijn verstrekt, zo spoedig mogelijk kennis te geven van de verbetering, aanvulling, verwijdering of afscherming, tenzij dit onmogelijk blijkt of onevenredige inspanning kost.
8. Een beslissing op een verzoek om inzage en een beslissing als vermeld in lid 4 van dit artikel zijn besluiten in de zin van de Algemene Wet Bestuursrecht.

Artikel 12 Bewaartermijnen
1. De persoonsgegevens worden door de verwerkingsverantwoordelijke bewaard tot drie jaar na afloop van:

a. de beoordeling van de toelaatbaarheid van de leerling tot het onderwijs aan een speciale school voor basisonderwijs in het samenwerkingsverband of tot het (voortgezet) speciaal onderwijs,
b. de advisering over de ondersteuningsbehoefte van de leerling aan het bevoegd gezag van de school waar de leerling is aangemeld of ingeschreven, of
c. de toewijzing van ondersteuningsmiddelen of ondersteuningsvoorzieningen aan de school, voor zover het voor die toewijzing nodig was gegevens van de leerling te verwerken.

2. De verwerkingsverantwoordelijke bewaart de gegevens op een plaats die uitsluitend toegankelijk is voor het samenwerkingsverband en de deskundigen, bedoeld in artikel 18a Wpo lid 11 en in artikel 17a Wvo lid 12.[4]

Artikel 13 Functionaris Gegevensbescherming
1. Het samenwerkingsverband wijst een Functionaris Gegevensbescherming aan die op basis van dienstverband of dienstverleningsovereenkomst de wettelijke taken verricht die horen bij deze functie.
2. De functionaris voor gegevensbescherming vervult ten minste de volgende taken:
a. de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van de AVG en overige wettelijke bepalingen;
b. toezien op naleving van de AVG en overige wettelijke bepalingen ten aanzien van bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
c. desgevraagd advies verstrekken met betrekking tot de privacy impact assessment (PIA) en toezien op de uitvoering daarvan in overeenstemming met de AVG;
d.met de Autoriteit Persoonsgegevens samenwerken en optreden als contactpunt voor de Autoriteit.

Artikel 14 Register Verwerkingsactiviteiten

Het samenwerkingsverband houdt een register van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens:

[4] Dit zijn de deskundigen die advies geven over de toelaatbaarheid van leerlingen tot het SBO of (V)SO zoals een orthopedagoog en door een tweede deskundige als een kinder- of jeugdpsycholoog, een pedagoog, een maatschappelijk werker, een arts of een kinderpsychiater.

a. de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken en van de functionaris voor gegevensbescherming;
b. de verwerkingsdoeleinden;
c. een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
d. de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
e. indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;
f. de beoogde termijnen (doorgaans 3 jaar) waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
g. een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen om de persoonsgegevens op een zorgvuldige wijze te verwerken.

Artikel 15 Datalekken
1. Bij een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4.12 van de AVG, wordt er melding gedaan bij de Functionaris Gegevensbescherming (FG) van het Samenwerkingsverband VO 2203.
2. De FG toetst deze inbreuk aan artikel 33 en 34 van de AVG en bepaald op basis van deze toetsing de vervolgstappen conform het protocol datalekken.

Artikel 16 Klachten
1. Als de betrokkene dan wel diens wettelijk vertegenwoordiger van mening is dat de bepalingen van de AVG zoals uitgewerkt in dit reglement niet worden nageleefd of andere redenen tot klagen heeft, dient hij zich te wenden tot de verwerkingsverantwoordelijke.
2. Overeenkomstig de AVG kan de betrokkene of diens wettelijk vertegenwoordiger zich wenden tot de rechter of de Autoriteit Persoonsgegevens.

Artikel 17 Slotbepalingen
1. Dit reglement kan aangehaald worden als “Privacyreglement verwerking persoonsgegevens SWV VO 2203” en treedt in werking op …… en vervangt daarmee de versie van.....
2. Het samenwerkingsverband maakt het reglement (digitaal) openbaar.

Bijlage 5: Zorgvuldigheidsverklaring persoonsgegevens

1. In het algemeen doe ik niets wat ongeoorloofde inbreuk op de persoonsgegeven betreft.
2. In ga zorgvuldig om met het delen van persoonsgegevens zoals e-mailadressen en persoonlijke telefoonnummers.
3. Ik laat wachtwoorden en/of persoonlijke toegangscodes en/of sleutels die aan mij verstrekt zijn in het kader van mijn werkzaamheden voor het SWV VO 2203 niet onbeheerd achter: ze zijn niet zichtbaar en/of toegankelijk en/of beschikbaar voor derden.
4. Wachtwoorden en toegangscodes zijn persoonlijk. Ik verstrek die niet aan derden. Tot het tegendeel bewezen is, ben ik persoonlijk verantwoordelijk voor de gevolgen, als een derde met behulp van mijn persoonlijke wachtwoord, zich toegang heeft verstrekt tot privacygevoelige gegevens.
5. Als ik mijn werkplek verlaat, vergrendel ik het beeldscherm van mijn computer (Windowstoets + L gelijktijdig indrukken).
6. Als ik afdrukken maak, gebruik ik altijd de aan mij verstrekte persoonlijke code.
7. Als ik afdrukken van documenten waarin privacygevoelige gegevens zijn opgenomen, laat ik de printer niet onbeheerd achter tijdens het afdrukken van die documenten.
8. Ik heb standaard uitsluitend toegang tot persoonsgegevens in het kader van mijn werkzaamheden voor het SWV VO 2203, via vaste personal computers.
9. Ik zorg ervoor dat de persoonsgegevens waarover ik in het kader van mijn werkzaamheden voor SWV VO 2203 kan beschikken, niet opgeslagen worden op portable devices zoals laptop, telefoon, usb-sticks, etc.);
10. Het SWV VO 2203 heeft een kantoor in het accountantskantoor Tamek.
11. Indien derden verblijven in het kantoor van het SWV VO 2203, dan is de directeur daarvan op de hoogte gesteld.
12. Derden die een afspraak hebben met een medewerker van het SWV VO 2203 gebruiken niet de kantoorruimten van SWV VO 2203 als wachtruimte.
13. Ik ga zorgvuldig om met e-mailadressen door, bij groepsmail, indien mogelijk gebruik te maken van „bcc" in plaats van „aan" of „cc".
14. Ik verstrek niet zonder meer e-mailadressen aan derden.
15. Ik neem in mijn e-mails een disclaimer op namelijk: *De inhoud van dit bericht is alleen bestemd voor de geadresseerde en kan vertrouwelijke of persoonlijke informatie bevatten. Als u dit bericht onbedoeld heeft ontvangen verzoeken wij u het te vernietigen en de afzender te informeren. Het is niet toegestaan om een bericht dat niet voor u bestemd is te vermenigvuldigen dan wel te verspreiden.*
16. Persoonsgegevens van leerlingen worden bij voorkeur via de beveiligde internetomgeving van het digitaal informatiesysteem (Grippa) van het SWV VO 2203 uitgewisseld of op een andere beveiligde manier.
17. Telefonisch wissel ik geen persoonsgegevens uit.

18. Als ik op een van de hierboven genoemde punten niet heb gehandeld volgens afspraak, meld ik dat aan directeur.
19. Als ik van mening ben dat er privacygevoelige informatie is gelekt binnen de eigen of een organisatie met wie beroepsmatig wordt samengewerkt, meld ik dat zo snel mogelijk maar in ieder geval binnen 24 uur bij de directeur en indien deze onbereikbaar is, bij de voorzitter van SWV VO 2203

Naam medewerker Functie

Datum Handtekening

Bijlage 6: Autorisatiematrix

Overzicht van functies die toegang hebben tot de in de verwerking opgenomen persoonsgegevens van stichting SWV VO 2203:

			GRIPPA			Bloemert ICT	
	Organisatie	**Functie**	**invoeren leerling**	**CAT**	**VO2203**	**CAT rechten**	**SWV**
	Scholen		x				
		Ondersteuningscoördinator / Intern Begeleider	x	x		x	
		Zorgcoördinator	x				
		Orthopedagoog	x				
		Directeur	x				
		Leerlingenadministratie					
		Vertrouwenspersoon	x				
		Ambulant begeleider	x				
		Onderwijskundige	x				
	CAT	psycholoog	x	x		x	
		orthopedagoog	x	x		x	
	SWV	directeur	x	x	x	x	x
		secretaresse	x	x	x	x	x
Extern | Grippa	Grippa				x		
Extern	Bloemert ICT						x
	Perspectief op school	Kwaliteit			x		

Bijlage 7: Bewaartermijnen

In het kader van de aangescherpte privacywetgeving is het goed archiveren van stukken, maar ook het vernietigen ervan nog belangrijker geworden.
In 2023 zal de nieuwe Archiefwet het mogelijk maken voor het onderwijs om bewaartermijnen voor de sector vast te stellen. Zodra de VO-Raad op basis van de nieuwe Archiefwet selectielijsten zal opstellen voor de sector zullen deze door SWV VO 2203 verwerkt worden.

Bijlage 8: Protocol gebruik bedrijfsmiddelen

1. Inleiding

Het gebruik van internet, computernetwerk, en e-mail is voor alle medewerkers van de school noodzakelijk om de werkzaamheden te kunnen verrichten. Bij deze werkzaamheden wordt gebruik gemaakt van veel gegevens, waaronder persoonsgegevens. De (ICT)faciliteiten en de verschillende gegevens worden in dit document **bedrijfsmiddelen** genoemd.

Onder bedrijfsmiddelen worden in ieder geval verstaan:

- **Hardware**: pc, laptop, tablet, telefoon, hardware token (tag).
- **Software (of -systemen)**: alle applicaties voor het uitvoeren van de werkzaamheden, zoals de school e-mailomgeving, Microsoft Office, administratiesystemen en (online)digitaal lesmateriaal maar ook apps op (mobiele) devices.
- **Informatie en (persoons)gegevens**: rapportages, leerling dossiers, gegevens in e-mails. Hierbij vraagt de verwerking van persoonsgegevens vanuit de privacywetgeving extra maatregelen.
- **Internetgebruik**: het bezoeken van het World Wide Web, het gebruik van e-mail en diensten als FTP en maar ook sociale media zoals Facebook, LinkedIn, Instagram en Twitter.

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers van SWV VO 2203 wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor de school uit te voeren.

De afspraken in dit document gelden voor alle locaties van waaruit (school)werkzaamheden worden verricht en voor alle devices waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij SWV VO 2203 ook voor uitzendkrachten en tijdelijke werknemers.

1.1. Uitgangspunten gedragscode

Deze gedragscode legt regels vast voor het gebruik van de bedrijfsmiddelen door medewerkers en over de controle op de naleving hiervan.
Het doel van deze gedragscode is om de normen en uitgangspunten vast te leggen ten aanzien van:

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

De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. SWV VO 2203 zal dan ook de controle en handhaving van deze regels conform de privacywetgeving en het algemene arbeidsrechtelijk kader uitvoeren. Hierbij is het uitgangspunt een goede balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers op de werkplek. Gegevens worden alleen verzameld en gebruikt voor deze doelen. In het bijzonder zal het bestuur de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang. Het bestuur zal mensen met toegang daartoe contractueel verplichten tot afdoende geheimhouding.

SWV VO 2203 streeft in het kader van handhaving van dit document naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele medewerkers zo veel mogelijk beperken. Zij zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in het gedrag van individuele personen.

1.2. Eigen verantwoordelijkheid en privégebruik

Het gebruik van door SWV VO 2203 verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle devices die voor schoolwerk worden gebruikt (inclusief eigen devices 'Own Device') worden niet uitgeleend of aan anderen ter beschikking gesteld zonder aanvullende (beveiligings)maatregelen. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen.

1.3. Verschillende soorten gegevens

SWV VO 2203 is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens.
SWV VO 2203 onderscheidt drie typen gegevens:

- **Openbare gegevens;** dit zijn gegevens die juist voor publicatie bedoeld zijn.
- **Interne gegevens**; dit zijn gegevens die alleen voor gebruik en verwerking binnen SWV VO 2203 bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- **Vertrouwelijke gegevens**; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen SWV VO 2203 toegankelijk zijn. Denk hierbij aan (bijzondere) persoonsgegevens, personeelsgegevens of aanbestedingsgegevens.

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

De privacywetgeving verplicht elk individu om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat SWV VO 2203 schriftelijk afspraken maakt met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk).

SWV VO 2203 heeft een Functionaris voor gegevensbescherming aangesteld. Deze communiceert intern de gedragsregels die horen bij het verwerken van persoonsgegevens. Persoonsgegevens moeten altijd met uiterste zorgvuldigheid verwerkt en gedeeld worden.

Als persoonsgegevens toegankelijk en of inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot deze gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en SWV VO 2203.
Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan SWV VO 2203 afspraken over:

- de verwerking en verspreiding van vertrouwelijke- en persoonsgegevens. Er worden niet meer gegevens verwerkt dan noodzakelijk om het doel te bereiken
- de uitwisseling van gegevens, waarbij aan de ontvanger wordt aangegeven wat de ontvanger wel of niet mag doen met de gegevens
- opslag en verspreiding van gegevens, waarbij alléén gebruik gemaakt wordt van door SWV VO 2203 goedgekeurde bedrijfsmiddelen.

Van medewerkers van SWV VO 2203 en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bv. personeelsdossiers, vertrouwelijke enquêtegegevens, zorgdossiers et cetera wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. Dat zij de privacywetgeving hanteren en op geen enkele wijze informatie, waarvan redelijkerwijze kan worden aangenomen dat deze vertrouwelijk of privacygevoelig is, zonder toestemming van betrokkene of leidinggevende te gebruiken en/of naar buiten te brengen.

2. Gedragscode

In deze gedragscode voor verantwoord gebruik van bedrijfsmiddelen geeft SWV VO 2203 aan wat de afspraken zijn met betrekking tot verschillende onderwerpen rondom het gebruik van bedrijfsmiddelen en wat dit voor de medewerkers in de dagelijkse praktijk betekent.

2.1. Algemene normen

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

- Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht.
- Voorkom het lekken van interne en vertrouwelijke informatie.
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen. (beveiligingsmaatregelen).
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild (bijvoorbeeld door jailbreaks).
- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering door het sturen van een e-mail aan evdwaeter@vo2203.nl of een telefonische melding bij de daarvoor aangewezen persoon (Zie hiervoor de procedure meldplicht datalekken van SWV VO 2203.

2.2. Computergebruik

Voor het uitoefenen van de werkzaamheden stelt SWV VO 2203 aan de medewerker computer- en netwerkfaciliteiten (ict-bedrijfsmiddelen) ter beschikking. Het gebruik van deze ict-bedrijfsmiddelen is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.
- Weet welke gegevens er mogen worden gebruikt (mag iedereen het zien?) en welke ict-voorzieningen kunnen worden ingezet (is het veilig genoeg?) bij het verrichten van de verschillende schoolwerkzaamheden.
- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op. (Opslaan van gegevens in public Cloud omgevingen, zoals een persoonlijke dropbox, is niet toegestaan).
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Sluit na gebruik de computer af of log uit.
- Meld storingen van beheerde werkplekken (computer of laptop) bij de ict-afdeling support@bloemert.com
- Werkplek
  Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen waartoe zij geen rechten hebben en/of laat gegevens niet (onbedoeld) lekken. Als aanvullende regels op computergebruik gelden voor de werkplek de volgende clean desk en clear screen regels:
- Vergrendel bij het tijdelijk verlaten van de werkplek de pc (windowstoets+L).
- Verwijder interne en vertrouwelijke documenten van het bureau bij het voor langere tijd verlaten van de werkplek (denk hieraan bij het bijwonen van een vergadering).
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via een beamer) mee kan kijken. Sluit het e-mail programma af en zorg voor een opgeruimd digitaal bureaublad.
- Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan.
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar.

LET OP: Als persoonsgegevens toegankelijk/inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot die gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Weet dat beveiligingsincidenten en mogelijke datalekken gemeld moeten worden volgens de procedure meldplicht datalekken van SWV VO 2203.

2.3. Gebruik eigen devices (BYOD)

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor SWV VO 2203 worden uitgevoerd. Het SWV VO 2203 is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van het samenwerkingsverband.
Voor 'Own Devices' ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

- Beveilig het device met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode die langer is dan 6 tekens.

- Vergrendel het device bij het verlaten van de werkplek (windowstoets+L).
- Sla persoonsgegevens van SWV VO 2203 niet op het eigen device op; dit is niet toegestaan.
- Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot SWV VO 2203 als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden (denk hierbij aan het eigen device of usb-stick).
- Scheid (versleutelde)gegevens, anders dan persoonsgegevens, van SWV VO 2203 en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen device.
- Houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks).
- Neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het periodiek (minimaal maandelijks) scannen van het device.

SWV VO 2203 mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van SWV VO 2203 moet de medewerker zelf aantonen dat de bovenstaande maatregelen worden toegepast.

2.4. Gebruik van e-mail

SWV VO 2203 stelt een e-mailsysteem en een bijbehorende mailbox aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik van e-mailfaciliteiten is verbonden aan deze werkzaamheden en gaan uit van de volgende afspraken:

- Gebruik het school e-mail adres *alléén* voor school gerelateerde zaken.
- Gebruik voor privé e-mail een eigen privé e-mailadres via een externe webmaildienst. (bijvoorbeeld webmail van Gmail, Hotmail of een eigen provider).
- Ontvangen van privémail op het vo2203 e-mailadres is incidenteel toegestaan.
- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.
- Het is niet toegestaan e-mail te gebruiken voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of voor berichten die kunnen aanzetten tot haat en geweld.
- Synchroniseert een medewerker de school e-mail met een eigen devices (tablet, telefoon) dan kan SWV VO 2203, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het device gewist worden.

2.5. Gebruik van internet

SWV VO 2203 stelt het gebruik van internet en de bijbehorende faciliteiten aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik hiervan is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

a. Beperkt persoonlijk gebruik is toegestaan, mits dit
   - niet storend is voor de dagelijkse werkzaamheden
   - niet voor commerciële doeleinden is en
   - geen verboden gebruik oplevert.

b. Het is niet toegestaan om
   - op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten
   - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron
   - onder lestijd internettoegang te gebruiken voor privédoeleinden
   - deel te nemen aan kansspelen.

c. Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale netwerken en andere vergelijkbare communicatienetwerken over alle aan school verbonden betrokkenen en activiteiten. Dit geldt in het bijzonder ook voor internetgebruik buiten het schoolnetwerk met betrekking tot aan de school verbonden betrokkenen en activiteiten.

2.6. Veilig online

Menselijk (online)handelen staat veelal aan de basis van een datalek.
SWV VO 2203 verwacht van medewerkers dat zij:

- het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken) en websites
- bij het verwerken van persoonsgegevens alléén gebruik maken van bekende én beveiligde draadloze netwerken
- weten wat malware is, het kunnen herkennen en weten hoe te handelen
- terughoudend zijn met het online achterlaten van gegevens met betrekking tot SWV VO 2203
- controleren of er daadwerkelijk van een bekend én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes. (Een netwerk kan bekend zijn omdat het een SWV VO 2203 netwerk is, eduroam of het eigen draadloze netwerk thuis is).

2.7. Sociale media

Sociale media is een verzamelnaam voor alle internettoepassingen die het mogelijk maken om informatie met elkaar te delen op een eenvoudige en vaak leuke manier. Het gaat hierbij niet alleen om informatie in de vorm van tekst (nieuws, artikelen). Ook geluid (podcasts, muziek) en beeld (fotografie, video) worden gedeeld via social media (Instagram, YouTube, Facebook, Twitter enz). De essentie van sociale media is dat iemand er informatie deelt over zichzelf, over anderen of over een bepaald onderwerp.
Voor gebruik van sociale media geldt als uitgangspunt dat het digitale gedrag op sociale media niet afwijkt van het real life gedrag binnen de school. Medewerkers zijn altijd de vertegenwoordiger van SWV VO 2203 ook als zij online een privémening verkondigen.
Bij SWV VO 2203 gelden de volgende afspraken voor het gebruik van sociale media:

- Deel op verantwoorde wijze kennis via sociale media rekening houdend met de goede naam van SWV VO 2203 en iedereen die hierbij betrokken is.
- Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens SWV VO 2203 gedaan wordt.
- Publiceer geen vertrouwelijke informatie op sociale media.
- Publiceer geen beeldmateriaal van leerlingen zonder de uitdrukkelijke voorafgaande aantoonbare toestemming van ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder is dan 16 jaar.
- Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn. Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren.
- Neem contact op met een leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met SWV VO 2203.
- Het is medewerkers niet toegestaan om met een privé account ‘vrienden’ te worden met leerlingen en ouders op sociale media.
- Inzetten van sociale media in het lesprogramma is gebonden aan de toestemming van ouders als leerlingen jonger zijn dan 16 jaar.

Aanvullende afspraken rondom social media in het algemeen zal het SWV VO 2203 vastleggen in een apart social mediaprotocol als daar aanleiding voor is.

2.8. Gebruik beeld- en geluidsmateriaal

Het gebruiken van beeld- en geluidsmateriaal, het delen van foto's, video's en geluidsfragmenten van leerlingen door medewerkers vallend onder SWV VO 2203 mag alleen als daar vooraf toestemming voor gegeven is door ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder dan 16 jaar is.
Zonder deze toestemming mogen geen foto's, video's en geluidsfragmenten van leerlingen gebruikt worden.

- SWV VO 2203 verwijst hierbij naar de richtlijn die is opgesteld voor het gebruik en toestemming van beeldmateriaal.
- Voor de afspraken rondom het delen van beeld- en geluidsmateriaal via sociale media gelden de richtlijnen die genoemd worden bij het gebruik van sociale media.
- Het beeldmateriaal wordt alleen gebruikt voor doeleinden waarvoor toestemming is gegeven.

2.9. Wachtwoorden en pincodes

Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en devices (pc, laptop, telefoon) begint met een goed wachtwoord. Een lang wachtwoord of een 'wachtzin' is beter dan een kort, complex wachtwoord. Voor het gebruik van wachtwoorden gelden onderstaande afspraken:

- Wachtwoorden moeten minimaal 8 tekens bevatten, met minstens drie van de volgende vier elementen : kleine letter, hoofdletter, cijfer of speciaal teken (!@#$%^&*()
- Pincodes (op telefoon of tablet) moeten langer zijn dan 4 tekens.
- Wachtwoorden moeten volgens de afspraken binnen SWV VO 2203 op aangegeven tijden vervangen worden.
- Gebruik niet voor elke systeem hetzelfde wachtwoord.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.

2.10. Meldplicht Datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens de procedure meldplicht datalekken van SWV VO 2203.

2.12 Werken op afstand

We werken steeds meer op afstand. Deze manier van werken heeft impact op de privacy van de medewerker en de wijze waarop we met elkaar omgaan.

Uitgangspunten:

- Zorg ervoor dat er geen privacygevoelige gegevens of andere personen ongewenst in beeld komen, zodra de camera aan staat;
- Bij voorkeur wordt de achtergrond vervaagt, middels de opties die de applicatie daarvoor biedt;
- Bij voorkeur wordt er een headset of koptelefoon gebruikt;
- Bij voorkeur wordt de microfoon gedempt. Als de microfoon aan staat, zorgt de spreker ervoor dat er geen privégesprekken of andere storende geluiden hoorbaar zijn;
- Bij voorkeur worden gesprekken niet opgenomen. Mocht dit toch nodig zijn dan dienen de gesprekdeelnemers te worden geïnformeerd over het doel en bewaartermijn van de opname. Deze opnames mogen niet openbaar gepubliceerd worden, niet met onbevoegden gedeeld worden en dienen na de afgesproken bewaartermijn verwijderd te worden.

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor SWV VO 22.03 worden uitgevoerd. SWV VO 22.03 is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen.

3. Controle gebruik bedrijfsmiddelen

SWV VO 2203 handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:

- De Grondwet,
- Algemene Verordening Gegevensbescherming
- Wet Medezeggenschap Onderwijs (WMO)
- Burgerlijk Wetboek (BW)
- Wetboek van Strafrecht
- Cao PO en
- Cao VO.

Het SWV VO 2203 zal bij controle rondom het gebruik van bedrijfsmiddelen op basis van deze gedragscode uitgaan van de juiste balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers.

3.1. Voorwaarden voor controle

- Controle van persoonsgegevens met betrekking tot gebruik van bedrijfsmiddelen vindt slechts plaats in het kader van handhaving van de doelen van deze gedragscode.
- Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
- Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode, in opdracht van SWV VO 2203 gerichte controle plaatsvinden.
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van SWV VO 2203, controle op de inhoud plaats.
- Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
- Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken medewerker besproken. SWV VO 2203 zal de medewerker op verzoek inzage verschaffen in de gegevens over het eigen gebruik. De medewerker wordt gewezen op de consequenties wanneer niet wordt gestopt met het ongeoorloofd gebruik.
- E-mailberichten van leden van de OPR onderling, van vertrouwenspersonen, bedrijfsartsen en van een ieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Dit geldt niet voor veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.

3.2. Uitvoering van de controle

- De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering.
- De controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.
- De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens.
- controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.
- De afdeling ict, de systeembeheerder(s) zijn aan geheimhouding gebonden als men om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.
- Door SWV VO 2203 worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- Door SWV VO 2203 worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

3.3. Disciplinaire maatregelen

Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het bestuur van SWV VO 2203 afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen. Hieronder vallen o.a. een waarschuwing/berisping, schadevergoeding, aangifte bij de politie, overplaatsing, schorsing en/of beëindiging van de arbeidsovereenkomst.
Medewerkers die zich niet aan deze gedragscode houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken. Zij krijgen daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. Medewerker en leidinggevende maken dan afspraken voor de toekomst en bepalen de mogelijke maatregelen bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in deze gedragscode bepaalde. Ook kan de toegang tot e-mail of internet worden beperkt of geheel

worden afgesloten. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens worden getroffen, zoals een constatering van een automatisch filter of blokkade. Er worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

3.4. Bezwaar en beroep

Als de medewerker het niet eens is met de (voorgenomen) disciplinaire maatregel, dan kan daar in een aantal gevallen bezwaar en/of beroep tegen worden ingesteld. Dit is meestal geregeld in de arbeidsovereenkomst, regels rondom personeelszaken en/of de van toepassing zijnde CAO.

4. OPR

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle
van het gedrag of de prestaties van medewerkers. Het medezeggenschapsorgaan (de OPR) is om deze reden instemmingsplichtig. De OPR heeft op <datum> ingestemd met de inhoud van deze gedragscode.
De organisatie kan deze gedragscode met instemming van de OPR wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering ervan aan de medewerkers bekend gemaakt.

5. Slotbepaling

Deze regeling wordt jaarlijks geëvalueerd door SWV VO 2203 en de OPR.
De eerstkomende evaluatie vindt plaats op .....