INFORMATIEBEVEILIGINGS- EN PRIVACYBELEID

STICHTING OPENBAAR ONDERWIJS ZWOLLE EN REGIO, MEI 2023

1. Belang IBP

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. Ook de voortgang van het onderwijs en het waarborgen van een optimale bedrijfsvoering is een belangrijk doel. In dit document is het IBP-beleid voor Openbaar Onderwijs Zwolle en Regio uitgewerkt.
Het IBP beleid is vastgesteld door het College van Bestuur d.d. 8 mei 2023, na instemming van de GMR- en PO, VO en SOVSO d.d. 18 april 2023 en treedt in werking d.d. 9 mei 2023.

2. Toelichting IBP

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 bedrijfs- voering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot schending van de privacy van betrokkenen, financiële schades en imagoverlies.

2.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de vigerende wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens ver- werkt 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 voor informatiebeveiliging en privacy binnen OOZ en vormt de kapstok voor de onderliggende afspraken en procedures.

2.4 Relevante wet- en regelgeving

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

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming
- Uitvoeringswet Algemene Verordening Gegevensbescherming
- Archiefwet
- Leerplichtwet 1969
- Auteurswet
- Wetboek van Strafrecht

Het normenkader voor informatiebeveiliging en privacy is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy'[1] zijn leidend bij het maken van afspraken met leveranciers. Dit betreft leveranciers die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

2.5 Basisregels omgaan 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 (er moet om toestemming gevraagd worden van de betrokken persoon; de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst, het nakomen van een wettelijke verplichting, ter bescherming van vitale belangen, voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag of voor de behartiging van de gerechtvaardigde belangen).
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

[1] https://www.privacyconvenant.nl/

niet met minder, alternatieve of andere gegevens worden bereikt (subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. Transparantie: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante 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.

3. Doel en reikwijdte IBP

3.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan OOZ persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers.
- 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 tus- sen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en OOZ voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

Het IBP-beleid van OOZ:

- Geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen alle devices binnen en buiten het beheer van OOZ van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen en buiten OOZ. Dit zijn in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing) en overige betrokkenen waarvan OOZ persoonsgegevens verwerkt.
- Geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van OOZ. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet- gecontroleerde informatie waarop de school kan worden aangesproken[2].
- Geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van OOZ. Ook geldt dit voor de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Daarnaast is het beleid ook van toepassing op niet- geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te

[2] Zie ook de gedragscodes personeel en leerlingen/ouders van OOZ.

worden opgenomen.

- Heeft binnen OOZ raakvlakken met:
  - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen (het OOZ Schoolveiligheidsplan).
  - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functie- wisselingen, functiescheiding en vertrouwensfuncties.
  - *ICT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
  - *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers.

4. Uitgangspunten IBP

OOZ hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het bestuur van OOZ neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld worden. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
2. OOZ voldoet aan alle relevante wet- en regelgeving.
3. Bij OOZ 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 OOZ 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 te allen tijde hun toestemming herzien.
4. OOZ informeert alle betrokkenen helder en actief 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. Bij wijziging van de privacy-voorwaarden, waarbij sprake is op een grotere inbreuk op de privacy van leerlingen en/of hun ouders wordt een mini-risicoscan uitgevoerd. Indien de uitkomst van de risicoscan daar aanleiding toe geeft worden de MR van de school en/of de leerlingen en hun ouders geïnformeerd.
6. OOZ legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. OOZ voldoet hiermee aan de documentatieplicht.
7. Binnen OOZ 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. Medewerkers hebben een geheimhoudingsplicht. De geheimhoudingsplicht geldt niet voor leerlingen, hun ouders en andere betrokkenen.
8. OOZ is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het intellectueel eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
9. OOZ classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risico-analyse 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.
10. OOZ sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school ,

persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt. Alle verwerkersovereenkomsten worden voor ondertekening centraal beoordeeld.

11. OOZ 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. OOZ heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
12. Informatiebeveiliging en privacy is bij OOZ een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
13. OOZ 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.
14. OOZ neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren. Door middel van autorisatiebeheer, het correct toewijzen van toegangsrechten aan personen, verkrijgen alleen degenen die daadwerkelijk bij gegevens moeten kunnen voor het uitvoeren van hun werkzaamheden de benodigde toegangsrechten .Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt OOZ aanvullende afspraken vast over de technische maatregelen, bijvoorbeeld in een (verwerkers)overeenkomst.
15. OOZ legt alle beveiligingsincidenten vast. OOZ legt datalekken vast en handelt deze af volgens een vast protocol. OOZ registreert incidenten en meldt deze bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

5. Uitwerking uitgangspunten IBP

Dit hoofdstuk geeft een praktische uitwerking van bovenstaande uitgangspunten.

5.1 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. In de onderstaande tabel staat een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen (in willekeurige volgorde).

Omschrijving	Opmerkingen
Beleidsstukken, richtlijnen en protocollen	
Privacyreglement medewerkers en leerlingen/ouders	Wordt herzien
Privacyverklaring	Wordt nog opgesteld
Privacystatement bezoekers website	
Informatiebeveiligingsbeleid (o.a. clear desk/screen, mobiele apparatuur, verwijderen bedrijfsmiddelen)	Wordt nog opgesteld
Beleid bewaren, archiveren en vernietigen persoonsgegevens (inclusief bewaartermijnen en beschrijving werkprocessen)	
Reglement cameratoezicht (inclusief voorwaarden inzetten of uitbreiden cameratoezicht)	Ontwikkeld, nog niet vastgesteld
Handboek en procedure datalekken	Wordt herzien
Gedragscode gebruik ICT middelen medewerkers en leerlingen	Wordt nog opgesteld
Social media protocol medewerkers en leerlingen	Wordt nog opgesteld

Omgaan met verschillende vormen van ouderlijk gezag	
Wachtwoordbeleid	
Back-up en restorebeleid	Wordt nog ontwikkeld
Procedures en werkprocessen	
Taakomschrijving FG	
Taakomschrijving privacy-ambassadeur	
Modelbrieven bij verzoek van een betrokkene	
Procedure veilig mailen	
Responsible disclosure	
Geheimhoudingsverklaring externen	
Toestemming beeldmateriaal leerlingen	
Procedure rechten betrokkenen	Wordt nog ontwikkeld
Procedure medewerkers uit dienst	Wordt nog ontwikkeld
Toestemming uitwisselen gegevens derden	Wordt nog ontwikkeld
Registers en DPIA's	
Register van verwerkingsactiviteiten	YourSafetyNet
Verwerkersovereenkomsten	YourSafetyNet
Register datalekken	Beheer externe FG
DPIA leerlingadministratiesystemen (SOMtoday, Magister, Parnassys)	In ontwikkeling
DPIA HR2day	Wordt nog ontwikkeld
DPIA Google Workspace for Education	Landelijk
DPIA's Microsoft	Landelijk
DPIA Cameratoezicht	Schoolniveau
Planning en evaluatie	
AVG audit 2020 en 2022	
IBP jaar- en activiteitenkalender	Wordt nog ontwikkeld
IBP actielijst 2022-2023	
Monitoren IBP beleid op schoolniveau	
Bewustwording	
Nieuwsbrieven directeuren	In ontwikkeling
Nieuwsbrieven medewerkers	In ontwikkeling
Nieuwsbrieven leerlingen (vanaf bovenbouw PO)	In ontwikkeling
Nieuwsbrieven ouders	In ontwikkeling

De aanvullende beleidsstukken, richtlijnen, procedures en protocollen worden periodiek geëvalueerd en indien nodig bijgesteld.
Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

5.2 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 bestuurssecretaris, de functionaris gegevensbescherming en de privacy functionaris, met het bestuur als eind- verantwoordelijke.

5.3 Classificatie, risicoanalyse en DPIA's

Alle informatie heeft waarde. Daarom worden alle gegevens en informatiesystemen waarop dit beleid van toe- passing 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 van belang.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen kijkt OOZ vooraf naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy. Hierdoor kan OOZ passende maatregelen nemen.

In bepaalde gevallen dient ook een DPIA uitgevoerd te worden. DPIA staat voor Data Protection Impact Assessment (gegevensbeschermings-effectenbeoordeling). Een DPIA is bedoeld om de privacyrisico's van een verwerking in kaart te brengen. Een DPIA is onder andere verplicht bij wijziging van gegevensverwerking of het aanvangen nieuwe gegevensverwerking en/of als een gegevensverwerking waarschijnlijk een hoog privacy risico oplevert voor de betrokkenen. Een DPIA legt vast wat de consequenties en risico's zijn van de verwerking voor de privacy van de betrokkenen. Op basis van de uitkomsten van het DPIA bepaalt OOZ of er (extra) maatregelen nodig zijn om de privacy van de betrokkenen (beter) te beschermen.

5.4 Incidenten en datalekken

Alle medewerkers 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. Medewerkers melden (beveiligings-)incidenten bij de functionaris voor gegevensbescherming, via fg@ooz.nl
Periodiek bespreekt OOZ beveiligingsincidenten en neemt waar nodig aanvullende passende beleidsmaat- regelen.

5.5 Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door de directeur bedrijfsvoering in samenwerking met de bestuurssecretaris en het IBP-kernteam en vastgesteld door het bestuur na instemming door de gmr. OOZ houdt hierbij rekening met:

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

Daarnaast kent OOZ een jaarlijkse planning- en controlcyclus 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 meegenomen. Het jaarplan wordt opgesteld door het IBP-kernteam.

5.6 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. Voor toezicht op de naleving van de AVG vervult de functionaris voor gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de het bestuur van OOZ en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. Mocht de naleving van dit beleid ernstig tekort schieten, dan kan OOZ de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.7 Logging en monitoring

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

6. Organisatie IBP

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 OOZ.

Rollen	Verantwoordelijkheid / taken	Realiseren / vastleggen

College van Bestuur	• Eindverantwoordelijk IBP inclusief besluitvorming nav PDCA
	• Besluiten nemen nav advies FG op bv incidenten, beleid
	• Aansturen crisisteam indien casus IBP/AVG zich voordoet zoals:
	  • Datalekken (met vele betrokkenen);
	  • Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
	  • Natuurrampen (brand, overstroming, storm, etc.).
	• Periodiek bespreken IBP met GMR.
		• Informatiebeveiligings- en privacy beleid vaststellen
		• Aanstelling FG

Directeur Bedrijfsvoering ism IBP-kernteam (dir BV 1e aanspreekpunt)	• Zorgen voor congruentie met (strategisch) OOZ-beleid, zowel in inhoud als planning • IBP- beleid beheren, uitvoeren en actualiseren en zorgen voor synergie en uniformiteit in uitvoering • Privacy team OOZ /organisatie IBP (inrichten/overleg voeren etc) • Algemene communicatie naar scholen (ism communicatie en IBP-kernteam) • Het beleid ism betrokken (Support-) medewerkers vertalen naar richtlijnen, procedures,	Informatie en beleid IBP, waaronder: • Activiteitenkalender OOZ (ism IBP-kernteam) • Beleid Informatie Beveiliging en Privacy (IBP) actueel houden • Actueel houden van IBP-protocollen en -reglementen, waar nodig juridisch advies aanwenden • Informatie OOZ op Mijn OOZ met privacy officer en FG actueel houden

	maatregelen, documenten • Participeren in crisisteam indien deze situatie zich voordoet	
Functionaris voor Gegevensbescherming (externe medewerker)	• Advisering IBP-kernteam en cvb • Advisering IBP-beleid/besluitvorming • Afhandelen vragen/klachten en datalekken • Onderzoeken organisatieonderdelen • Betrokken worden bij DPIA en beoordelen Verwerkingsregister • Voorlichting • Uitvoering Audits • Rapportages cvb • Contact met AP, indien nodig	Alle documentatie die voor kolom 2 nodig is. Bv (afhandeling) datalekken registeren in betreffende omgeving, audit-/evaluatierapportages schrijven, voorlichtingsmateriaal maken en bijhouden etc
Privacy Functionaris (interne medewerker (-s)van Support)	• Frontoffice voor FG, 1e afhandeling mailbox FG • Bijdrages aan IBP- beleid en uitvoering/evaluatie • "ICT-technisch/infrastructureel ''aanspreekpunt • Verwerkersovereenkomsten • Lid IBP-kernteam OOZ	Alle documentatie die voor kolom 2 nodig is. Bv (afhandeling) datalekken registeren in betreffende omgeving en verwerkersovereenkomsten documenteren.
Medewerkers Support	• IBP-beleid uitvoeren • Zorgvuldig omgaan met gegevens medewerkers in en uit dienst • Indien een medewerker eigenaar is van een werkproces, dit IBP-proof inrichten en bijhouden. • Veilig mailen en extra alert zijn bij bv HR-gegevens, financiële gegevens	• Alle documentatie die voor kolom 2 nodig is. Bv documenteren wie toegang heeft tot applicaties, waar van toepassing een procesbeschrijving maken en actueel houden.
Beenders applicaties	• Persoonsgegevens in applicaties AVG-proof inrichten. • Verwerkersovereenkomst applicatie regelen via IBP kernteam. • PDCA toegangsbeleid	• Zorgen dat de AVG voor wat betreft persoonsgegevens goed ingericht wordt in de applicatie • Zorgen voor een verwerkersovereenkomst via het IBP kernteam • Toegangsbeleid goed inregelen en documenteren en waar nodig controleren
Directeur / leidinggevende / teamleider/locatieleider etc.	• Toezien op de naleving van het OOZ-IBP- beleid in de school • Bij grotere scholen: zorgen voor domeinverantwoordelijkheden en proces-eigenaren IBP onderdelen. • Voorbeeldfunctie met positieve/actieve houding t.a.v. IBP-beleid. • Periodiek het onderwerp informatie- beveiliging onder de aandacht te brengen in de school • Bij incidenten/datalekken regierol namens de school nemen (ism bv andere MT-leden, ICT-	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerlingdossiers • Wie mogen wat zien • Gedragscode en omgaan sociale media • Mediawijs maken Voor de verschillende domeinen/processen, zoals ict, personeel, (ll.)administratie Op elk van deze domeinen/processen is iemand

	coördinatoren	verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.
IBP-verantwoordelijke school	Elke school heeft een IBP-verantwoordelijke (de directeur van de school of andere functionaris). Dit is een privacy contactpersoon / ambassadeur per (school-)locatie	• Eerste aanspreekpunt voor IBP-kernteam • Maakt hiervoor gebruik van de IBP-applicatie (vanaf 2023: Your Safety Net)
OOZ-Medewerker	Verantwoordelijk omgaan met IBP bij zijn of haar dagelijkse werkzaamheden. Dit betekent oa: • Zorgvuldig omgaan met persoonsgegevens en veilig mailen • MFA gebruiken • Clean desk o.a. spullen met persoonsgegevens niet onbeheerd neerleggen • In de cloud werken en dus niet op USB-sticks, bureaublad • Vertrouwelijke papieren in speciale papiercontainer weggooien • Veilig printen, kopiëren en scannen. • Wachtwoord -hygiëne opvolgen; MFA indien aanbevolen, sterk wachtwoord, regelmatig nieuw wachtwoord. • Computer /laptop/I-pad locken als medewerker wegloopt van werkplek	