



NORMEN KADER IBP

Informatiebeveiligings- en privacy beleid

Colofon

Versie Versie 1.0, oktober 2024

Normen

- BL.01** Privacybeleid
- BL.02** Rollen, taken en verantwoordelijkheden
- OR.01** Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid
- OR.02** Functiescheiding (gedeeltelijk)
- OI.02** Privacy organisatie
- OI.03** Betrokkenheid medezeggenschap
- GO.01** Strategie informatiebeveiliging
- GO.02** Beleid informatiebeveiliging

Auteurs Dit document is voor VRtL opgesteld door Bert Wolthuis (manager IBP) en Hugo van der Vlist (secretaris VRtL).

VRtL Van Reest tot Linde (VRtL) is een samenwerking tussen Simant en VOMEO.

Van Reest tot Linde werd als vereniging in het leven geroepen met als doelstelling om meer kwaliteit en besparingen te realiseren. Dit met in gedachte een verwachte krimp en het steeds zoeken naar mogelijkheden om middelen zo veel mogelijk direct voor het onderwijs in te zetten. Tegelijkertijd kan daarmee de kwetsbaarheid bij afnemende formatie worden tegengegaan en de uitwisseling van kennis en deskundigheid worden bevorderd waardoor ook verbreding en verdieping van taken ontstaat.

We trekken in VRtL verband samen op om het normenkader IBP in te voeren om zo digitaal veilige scholen te realiseren.

Documenthistorie

Versie	Datum	Auteur	Wijzigingen/ opmerkingen
0.1	12-06-2024	Hugo van der Vlist en Bert Wolthuis	Eerste opzet
0.2	25-6-2024	Hugo van der Vlist en Bert Wolthuis	Aanpassingen inleiding en praktische invulling van beleid
0.3	24-9-2024	Hugo van der Vlist en Bert Wolthuis	Kleine redactionele wijzigingen Toevoegen colofon; visie en strategie; instemmingsoverzicht IBP door GMR Voorstel rollen en verantwoordelijkheden
0.4	09-10-2024	Hugo van der Vlist en Bert Wolthuis	Besproken in Kernteam, kleine aanpassingen
0.5	11-10-2024	Hugo van der Vlist en Bert Wolthuis	Aanvullende controle norm OR.01 norm OR.02 functiescheiding wordt in het IBP-beleidsplan op niveau 2 vastgesteld (formele vaststelling)
0.6	21-10-2024	Hugo van der Vlist en Bert Wolthuis	Besproken in bestuurdersoverleg, kleine aanpassingen Toevoeging normen in kantlijn Versie 1.0 status
Versie	Datum	Distributielijst	Autorisatie
1.0	17-12-2024		Bestuurder VOMEQ: dhr. P.A. de Visser
Versie	Datum	Recht	Medezeggenschap
1.0	16-12-2024	Instemming	Bespreek- en beslisdocument voor de GMR Voorzitter GMR: dhr. B. van Dam

Inhoudsopgave

Inleiding	4
Hoofdstuk 1: Informatiebeveiliging en privacy	6
1.1 Vervlechting informatiebeveiliging en privacy: IBP	6
1.2 Doelen IBP	7
1.3 Reikwijdte	7
Hoofdstuk 2: Visie en strategie	8
2.1 Visie	8
2.2 Strategie	8
2.3 Projectorganisatie normenkader	8
2.4 Zeggenschap en medezeggenschap	9
2.5 Rol van de GMR	9
Hoofdstuk 3: Het beveiligen van persoonsgegevens	10
3.1 Beveiligen van gegevens	10
3.2 Verantwoordingsplicht	10
Hoofdstuk 4: Uitgangspunten voor IBP beleid	11
Hoofdstuk 5: Praktische invulling van beleid	12
5.1 Relevante wet- en regelgeving	12
5.2 Basisregels bij het omgaan met persoonsgegevens	12
5.3 Ondersteunende richtlijnen en procedures	13
5.4 Voorlichting en bewustzijn	13
5.5 Classificatie en risicoanalyse	13
5.6 Incidenten en datalekken	14
5.7 Planning en controle	14
5.8 Logging en monitoring	15
5.9 Audits en externe controle	15
5.10 Naleving en sancties	15
Hoofdstuk 6: Rollen en verantwoordelijkheden	16
6.1 Strategisch-, tactisch- en operationeel niveau	16
6.2 Overzicht rollen en verantwoordelijkheden	18
Bijlage 1: Uitwerkingen van mogelijke maatregelen	20

Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ict. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door ontwikkelingen binnen zowel de automatisering, het onderwijs als de regelgeving. 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 belangrijk, 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.

IBP gaat in eerste instantie niet om de organisatorische- en technische maatregelen, niet om ict, maar om gedrag, cultuur en bewustwording. Iedereen moet het IBP-beleid kunnen lezen, begrijpen en toepassen. Het IBP-beleid regelt de verantwoordelijkheden en de verschillende rollen binnen de school. Daarnaast wordt in dit beleid aangegeven welke organisatorische- en technische maatregelen de school treft om de informatie en privacy zo adequaat mogelijk te beschermen.

VOMEEO wil een veilige en professionele leer- en werkomgeving bieden waarin hoogwaardig onderwijs wordt gegeven. Daarvoor is het noodzakelijk dat de door VOMEEO verzamelde, verwerkte en gepubliceerde gegevens te allen tijde beschikbaar, correct en beschermd zijn. Om dit te realiseren worden (aanvullende) maatregelen op basis van het Normenkader Informatiebeveiliging en Privacy van OCW ingevoerd. Eind 2027 moeten al deze maatregelen zijn geïmplementeerd en moet hier bewust naar worden gehandeld. Het beleidsplan IBP geeft hieraan richting.

In de hoofdstukken 1 en 2 worden de definities voor informatiebeleid en privacy bepaald, daarbij worden de doelen en reikwijdte van dit beleidsplan beschreven. De hoofdstukken 3 t/m 6 gaan over beleid; de visie en strategie, de uitgangspunten die we hanteren, de beleidsmatige uitwerking en de rollen en verantwoordelijkheden van de verschillende medewerkers.

In bijlage 1 staan voorbeelden van organisatorische- en technische beveiligingsmaatregelen.

Dit beleidsplan maakt deel uit van de PDCA cyclus rondom het normenkader en wordt in principe elke drie jaar getoetst en bijgesteld.

De GMR heeft d.d. 16 december 2024 ingestemd met dit voorgenomen besluit.

Hoofdstuk 1: Informatiebeveiliging en privacy

GO.01
Informatiebeveiligingsbeleid is vastgesteld door het schoolbestuur

In dit hoofdstuk wordt beschreven welke definities we hanteren voor informatiebeveiliging en privacy. Deze definities zijn niet vrijblijvend, maar vrij strikt omschreven. Dit is waar we ons aan moeten houden en wat we moeten beveiligen.

1.1 Vervlechting informatiebeveiliging en privacy: IBP

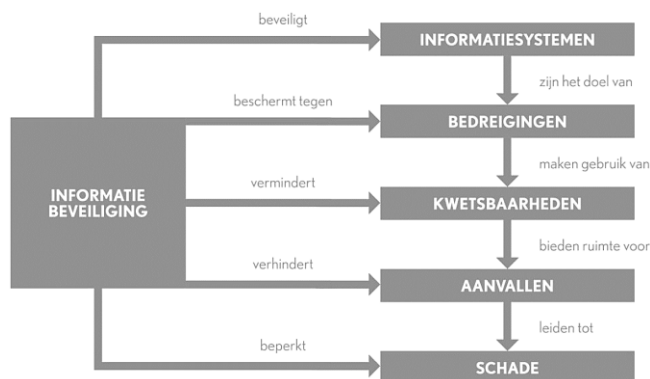
Informatiebeveiliging is een belangrijke voorwaarde voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Het IBP-beleid vormt de basis voor informatiebeveiliging en privacy binnen VOMEIO en vormt de kapstok voor de onderliggende afspraken en procedures.

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.



Privacy

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

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

1.2 Doelen IBP

Het IBP-beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkenen, waaronder medewerkers, leerlingen en hun ouders/verzorgers, wordt gerespecteerd en dat VOMEO voldoet aan relevante wet- en regelgeving.

Informatiebeveiliging en privacy heeft de volgende doelen:

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

1.3 Reikwijdte

De reikwijdte van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van VOMEO, het gebruik daarvan door medewerkers, leerlingen en ouders/verzorgers en partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

- Het IBP-beleid geldt in elk geval voor alle medewerkers, vrijwilligers, stagiairs, sollicitanten, leerlingen, ouders/verzorgers, bezoekers en externe partijen (bijvoorbeeld inhuur, outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle hierboven genoemde betrokkenen, evenals op overige betrokkenen van wie VOMEO persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het bestuur van VOMEO. Hieronder valt tevens de gecontroleerde informatie, die door de VOMEO zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken (bijvoorbeeld uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of sociale media).
- Het IBP-beleid geldt voor de geheel, of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van VOMEO 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 raakvlakken met:

- *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, crisismanagement, fysieke toegang en beveiliging, en huisvesting.
- *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
- *Onderwijs en begeleiding;* met als aandachtspunten de in- en uitschrijving van leerlingen, uitwisselen van informatie met scholen en instanties.
- *ICT-beleid;* met als aandachtspunten autorisatie, aanschaf, beheer en gebruik van ict en (digitale) leermiddelen.
- *Medezeggenschap* door leerlingen, hun ouders/verzorgers en medewerkers.

Hoofdstuk 2: Visie en strategie

2.1 Visie

GO.01
Strategie en visie op informatiebeveiliging zijn vastgesteld door het

VOMEO wil een veilige en professionele leer- en werkomgeving bieden waarin hoogwaardig onderwijs wordt gegeven. Daarvoor is het noodzakelijk dat de door VOMEO verzamelde, verwerkte en gepubliceerde gegevens te allen tijde beschikbaar, correct en beschermd zijn.

2.2 Strategie

OR.01
Op organisatieniveau zijn de verantwoordelijkheid en aansprakelijkheid voor risico- en informatiebeveiligingsmanagement vastgesteld.

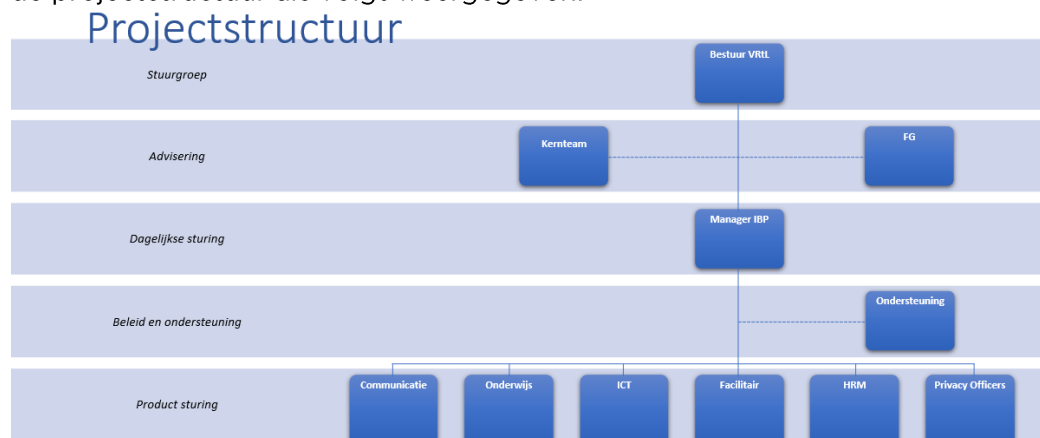
We willen groeien naar een professioneel volwassen organisatie, waar op een veilige manier onderwijs verzorgd en ondersteund kan worden en waar we op een veilige manier met informatie omgaan. Om dit te realiseren worden de (aanvullende) maatregelen op basis van het normenkader IBP ingevoerd. Eind 2027 moeten deze maatregelen zijn geïmplementeerd en moet hier bewust naar worden gehandeld.

Hiermee hebben we het volgende op het oog:

- Iedere medewerker is verantwoordelijk voor de veiligheid van de informatie die door de organisatie beschikbaar wordt gesteld.
- Alle leidinggevendenden zien erop toe dat hun medewerkers voldoende geschoold zijn en het Informatiebeveiliging en Privacy beleid naleven.
- Het College van Bestuur is eindverantwoordelijk en moet verantwoording kunnen afleggen aan, bijvoorbeeld, de Raad van Toezicht en de Autoriteit Persoonsgegevens.
- Proceseigenaren zijn benoemd en zijn bewust van hun verantwoordelijkheid bij de uitvoer van processen waar Informatiebeveiliging en Privacy een belangrijke rol speelt.
- IT is verantwoordelijk voor de technische weerbaarheid.

2.3 Projectorganisatie normenkader

Voor de implementatie van het Normenkader is een projectstructuur vastgesteld door het College van Bestuur, de bestuurder. Er is een zestal projectgroepen waarin de domeinverantwoordelijke/proceseigenaar zorgdraagt voor de implementatie en uitvoer van voor de projectgroep relevante normen uit het normenkader IBP. De sturing van dit project is in handen van de manager IBP. Er is voorzien in interne- en externe advisering van zowel de stuurgroep als de manager IBP. Schematisch is de projectstructuur als volgt weergegeven:



2.4 Zeggenschap en medezeggenschap

IBP moeten we gezamenlijk uitvoeren, daarom is het bij de ontwikkeling van beleid van belang om zoveel mogelijk medewerkers binnen de verschillende domeinen te betrekken. De gekozen projectstructuur draagt zorg voor het inhoudelijk betrekken van deze medewerkers. In de werkgroepen kan discussie plaatsvinden en beleid voorgesteld worden zodat we gezamenlijk het normenkader IBP tot een succes kunnen brengen.

Er is een formele rol voor de GMR. Vanwege de complexiteit van het normenkader wordt deze rol apart uitgewerkt, voorzien van een lijst met documenten waar de GMR een instemmingsbevoegdheid voor heeft.

2.5 Rol van de GMR

OI.03
Er is een gedocumenteerd proces dat specificeert hoe en wanneer de GMR geïnformeerd en betrokken wordt bij wettelijke taken op het gebied van privacy.

Personeel, ouders en in het voortgezet onderwijs ook leerlingen, kunnen meepraten over en invloed uitoefenen op het beleid van de school. De WMS kent in dat kader rechten en bevoegdheden toe aan (G)MR. De bevoegdheden bestaan uit instemmings- en adviesbevoegdheden. Daarnaast regelt de WMS een recht op overleg, het initiatiefrecht en het recht op informatie.

De (G)MR zou in het kader van haar initiatiefrecht voorstellen kunnen doen met betrekking tot de naleving van de AVG of het IBP-beleid of hier vragen over stellen. Het recht op informatie brengt met zich mee dat de (G)MR geïnformeerd wordt over AVG-gelegenheden, bijvoorbeeld over de afhandeling van een (groot) datalek. Bij de adviesbevoegdheden wordt in de wet geen specifieke verwijzing gemaakt naar IBP-onderwerpen. Wel kunnen deze onderdeel uitmaken van een adviesvraag die betrekking heeft op bijvoorbeeld het beleid met betrekking tot de organisatie van school, een onderwijskundig project of de samenwerking met een andere instelling. Het instemmingsrecht wordt verder uitgewerkt in artikel 12, 13 en 14 van de WMS. Volgens deze artikelen heeft (een geleding van) de medezeggenschapsraad het recht van instemming bij nieuwe of gewijzigde regelingen die betrekking hebben op het verwerken en beschermen van persoonsgegevens. Daarnaast wordt specifiek de vaststelling of wijziging van een regeling genoemd inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van het personeel. In de praktijk betreft het in ieder geval de volgende regelingen:

- IBP-beleid
- Gedragscode
- Privacyreglement
- Privacyverklaring
- Reglement, taken en bevoegdheden FG, alleen als de functie wordt toegevoegd aan het functiehuis
- Gedragscode m.b.t. gebruik ICT middelen
- Protocol datalekken
- Procedure DPIA
- Procedure en formulier gebruik beeldmateriaal
- Protocol sociale media
- Bewaartermijnenprotocol
- Archief- en vernietigingsbeleid
- Geheimhoudingsverklaring
- Beleid/reglement cameratoezicht
- Procedure uitwisseling persoonsgegevens en samenwerkingsovereenkomst
- Toegangs- / autorisatiebeleid
- Procedure klachten en rechten van betrokkenen

Hoofdstuk 3: Het beveiligen van persoonsgegevens

3.1 Beveiligen van gegevens

In de AVG staat dat persoonsgegevens goed beveiligd moeten worden. Dat betekent dat de school een overzicht moet hebben van de verwerkingen die uitgevoerd worden. Daarnaast moet bepaald worden welke technische en organisatorische maatregelen nodig zijn om die verwerkingen goed te beveiligen.

Het beveiligingsniveau moet afgestemd zijn op de risico's die de gegevensverwerking met zich meebrengt. Bijvoorbeeld risico's door vernietiging, verlies, wijziging of ongeoorloofde verwerking van persoonsgegevens. Daarbij wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, de aard en omvang van de verwerking en hoe waarschijnlijk en ernstig het is voor betrokkenen als er een beveiligingslek ontstaat.

Het is belangrijk om maatregelen te treffen die nodig zijn om:

- de vertrouwelijkheid, integriteit, beschikbaarheid van de verwerkingssystemen en diensten te garanderen;
- bij een incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- om met vaste regelmaat (tenminste éénmaal per jaar) te testen of de genomen beveiligingsmaatregelen voldoende effectief zijn.

3.2 Verantwoordingsplicht

Onder de AVG geldt een verantwoordingsplicht. Het bestuur moet kunnen aantonen dat er voldoende organisatorische- en technische maatregelen zijn genomen om de verwerkte persoonsgegevens te beveiligen. De Autoriteit Persoonsgegevens kan hiernaar vragen. Hieronder worden een aantal mogelijke maatregelen geschetst.

Voorbeelden van organisatorische maatregelen:

- Toewijzen van verantwoordelijkheden voor informatiebeveiliging.
- Bevorderen van beveiligingsbewustzijn bij bestaande en nieuwe medewerkers.
- Procedures om op gezette tijdstippen de beveiligingsmaatregelen te testen, te beoordelen en te evalueren.
- Regelmatige controle van de logbestanden.
- Een protocol voor de afhandeling van datalekken en beveiligingsincidenten.
- Afsluiten van verwerkersovereenkomsten en opstellen van een register van verwerkingen.
- Minder mensen in uw organisatie toegang geven tot persoonsgegevens.
- Het uitvoeren van een data protection impact assesment (DPIA).

Voorbeelden van technische maatregelen:

- Logische en fysieke (toegangs-)beveiliging van apparatuur.
- Technisch beheer van de autorisaties en bijhouden van logbestanden;
- Beheer van technische kwetsbaarheden (patch management).
- Software, zoals browsers, virusscanners en operating systems up-to- date houden.
- Een adequate back-up waarmee u de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig kunt herstellen.
- Automatisch verwijderen van verouderde gegevens.
- Versleuteling van gegevens.
- Pseudonimiseren van persoonsgegevens.

Hoofdstuk 4: Uitgangspunten voor IBP beleid

BL.01
Het privacybeleid is actueel en beschrijft hoe de organisatie uitvoering geeft aan de privacybeginselen die in art 5 lid 1 AVG zijn vastgelegd.

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

1. We nemen de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. De bestuurder is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is de bestuurder de verwerkingsverantwoordelijke.
2. Binnen de school 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.
3. We verwachten van alle medewerkers, leerlingen en andere betrokkenen dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. De school heeft hiervoor meerdere gedragscodes geformuleerd, waaronder het schoolstatuut, de gedrags- en integriteitscode en het reglement voor sociale media.
4. We voldoen aan de relevante wet- en regelgeving.
5. De verwerking van persoonsgegevens is altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van de school 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 verwerkingen van persoonsgegevens op basis van toestemming, kunnen betrokkenen te allen tijde hun toestemming herzien.
6. We informeren betrokkenen actief over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden de betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
7. We leggen alle verwerkingen van persoonsgegevens vast in een dataregister en houden deze up-to-date. Met regelmaat (tenminste eenmaal per jaar) wordt het dataregister gecontroleerd.
8. We classificeren informatie en informatiesystemen volgens bijvoorbeeld het BIV model. 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. We sluiten met alle leveranciers verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. De verwerkersovereenkomsten worden centraal beheerd.
10. Informatiebeveiliging en privacy is een continu proces, waarbij tenminste eenmaal per jaar wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
11. Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen kijken we vóóraf naar de impact hiervan op de informatiebeveiliging en privacy. Hierdoor kunnen tijdig de juiste maatregelen genomen worden.
12. We nemen passende organisatorische- en technische 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.
13. VOMEO is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd.
14. We handelen beveiligingsincidenten en datalekken af volgens een vast protocol en in voorkomende gevallen melden we bij de Autoriteit Persoonsgegevens en aan de betrokkenen.

Hoofdstuk 5: Praktische invulling van beleid

BL.01

Het privacybeleid beschrijft de verplichtingen zoals doelbinding, rechtmatigheid, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid die op de organisatie rusten op grond van relevante privacywetgeving en beschrijft hoe de organisatie uitvoering geeft aan deze verplichtingen.

Dit hoofdstuk geeft een praktische invulling van in hoofdstuk 4 genoemde uitgangspunten 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 VO
- Wet op het onderwijstoezicht
- Algemene Verordening Gegevensbescherming
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Het normenkader IBP voor Funderend Onderwijs (OCW, VO-raad, Sison en Kennisnet) is hierop gebaseerd en 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 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, genoemd in de AVG.
3. Dataminimalisatie: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Dit betekent ook dat data niet langer worden 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.

5.3 Ondersteunende richtlijnen en procedures

Diverse aanvullende maatregelen (in de vorm van beleidsstukken, richtlijnen, procedures en protocollen) geven invulling en gaan invulling geven aan de uitwerking van dit beleidsplan. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een register voor verwerkingen.

5.4 Voorlichting en bewustzijn

Beleid en maatregelen alleen, zijn niet voldoende om risico's uit te sluiten. De mens is hier ook een belangrijke factor. Gedrag is daarbij belangrijker dan kennis. Onderdeel van het beleid is dat medewerkers geschoold worden en dat er via bijvoorbeeld posters en nieuwsbrieven regelmatig aandacht is voor IBP. Voor leerlingen is het van belang dat er aandacht wordt besteed aan het veilig omgaan met persoonsgegevens. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de Privacy Officer en de direct leidinggevenden met de bestuurder als eindverantwoordelijke. De manager IBP en de FG kunnen hierbij ondersteunend zijn.

5.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden de gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd volgens bijvoorbeeld de BIV-classificatie. 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. Bij de start van nieuwe (ict-) projecten wordt rekening gehouden met informatiebeveiliging en privacy.

Niveau	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Laag	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meerdere dagen brengt geen merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.	Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn. Indien informatie niet correct is, leidt dit tot beperkte schade.	Openbaar worden van gegevens leidt tot weinig of geen schade voor een instelling of betrokkene.
Midden	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een dag brengt beperkte schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.	Blijvende juistheid van informatie moet gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden.	De organisatie, instelling of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun

		Indien informatie niet correct is, kan de organisatie wel een substantiële schade lijden.	functie toegang toe moeten hebben (need-to-know basis). Hieronder vallen onder andere persoonsgegevens.
Hoog	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.	Informatie moet gegarandeerd correct zijn. Informatie waarbij het noodzakelijk is dat de correctheid niet betwist kan worden, zoals de uitslagen van toetsen, examens, onomkeerbare financiële transacties. Indien informatie niet correct is, kan de organisatie ernstige schade lijden.	De organisatie, instelling of betrokkene kan ernstige schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer geselecteerde groep personen. Hieronder vallen onder andere bijzondere persoonsgegevens.

5.6 Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden, dienen dit te melden bij de Privacy Officer en de direct leidinggevende. Meldingen worden geregistreerd. De functionaris voor de gegevensbescherming rapporteert jaarlijks hierover. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een beleidsplan datalekken. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. De beveiligingsincidenten worden vastgelegd in een incidentenregister. Het incidentenregister wordt gebruikt om van te leren en om incidenten in de toekomst te minimaliseren: periodiek (tenminste éénmaal per jaar) zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7 Planning en controle

Het IBP-beleid wordt minimaal elke drie jaar getoetst en bijgesteld door de bestuurder. Hierbij wordt rekening gehouden met:

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

Daarnaast is er 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 worden getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen. Het jaarverslag van de FG zal deel uitmaken van deze evaluatie.

5.8 Logging en monitoring

Logging en monitoring door ICT zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens worden vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en pogingen tot ongeautoriseerde toegang tot het netwerk.

5.9 Audits en externe controle

Naast de toezichthouden rol van de FG wordt er met regelmaat onafhankelijk onderzoek gedaan naar de correcte uitvoering van IBP, bijvoorbeeld in de vorm van een accountantsonderzoek, een penetratietest of een onafhankelijk onderzoek naar de werking en veiligheid van de digitale infrastructuur.

5.10 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 mensen aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling en tijdens de gesprekkencyclus. Daarnaast wordt er in algemene zin aandacht besteed aan scholing en bewustzijn.

Voor toezicht op de naleving van de AVG vervult de FG (functionaris voor de gegevensbescherming) een belangrijke rol. De FG wordt aangesteld door de bestuurder 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 IBP-beleid ernstig tekortschieten, dan kan de school de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de cao-VO en de wettelijke mogelijkheden.

Hoofdstuk 6: Rollen en verantwoordelijkheden

BL.02

Rollen, taken en verantwoordelijkheden met betrekking tot privacy zijn formeel benoemd, belegd en vastgelegd in het privacybeleid en organisatie-breed bekend.

Vastgelegd is dat het schoolbestuur eindverantwoordelijk is voor privacy binnen de organisatie en dat managers verantwoordelijk zijn voor privacy binnen hun managementdomein.

OR.02

De scheiding van verantwoordelijkheden is vastgesteld door het schoolbestuur of de schoolleiding.

6.1 Strategisch-, tactisch- en operationeel niveau

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

Strategisch niveau (richtinggevend)

De bestuurder 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 manager IBP.

Tactisch niveau (sturend)

Manager IBP

Manager IBP is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de bestuurder en stuurt de mensen aan op uitvoerend niveau. De manager IBP moet:

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

Teamleider ICT

Adviseert samen met de manager IBP de bestuurder en is verantwoordelijk voor het organiseren van ict en informatiebeveiliging binnen de stichting VRtL.

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) 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 bestuurder. De FG heeft regelmatig overleg met de manager IBP en de Privacy Officers. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Privacy Officer

Per school is sprake van een Privacy Officer die uitvoering geeft aan het IBP-beleid van de school. Hij/zij ziet toe op de naleving van de AVG-wetgeving binnen de organisatie en draagt er (mede) zorg voor dat persoonsgegevens in veilige handen zijn. Hij/zij draagt tevens de zorg voor de bewustwording, het gedrag en het handelen op de werkvloer. De Privacy Officer adviseert gevraagd en ongevraagd over vraagstukken op het gebied van privacy en participeert in het coördinerend overleg van de Privacy Officers van de stichtingen VOME0 en Simant.

Domeinverantwoordelijke/proceseigenaar

Binnen VOMEO zijn er verschillende domeinen te onderscheiden, waaronder communicatie, onderwijs, ict, facilitair en HRM (personeel, administratie en financiën). Op elk van deze domeinen is iemand verantwoordelijk voor uitvoering van IBP beleid.

De domeinverantwoordelijke/ proceseigenaar is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- Samen met de manager IBP stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met ICT zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met facilitair, HRM en ICT beoordelen zij periodiek (tenminste eenmaal per jaar) de toegangsrechten van de gebruikers. Hierbij wordt specifiek gelet op in- en uitdiensttreding.

Operationeel niveau (uitvoerend)

Systeem- en netwerkbeheerder

De systeem- en netwerkbeheerder VRtL en de ICT op schoolniveau vormen een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Applicatiebeheerder

Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De applicatiebeheerder werkt vanuit een vooraf 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 o.a. beschreven in het privacyreglement, ict-reglement en de cao-vo.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van beveiligingsincidenten, datalekken, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).

Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- Ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid;
- Toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- Periodiek het onderwerp IBP onder de aandacht te brengen tijdens de gesprekken cyclus, maar ook tijdens werkoverleggen, beoordelingen etc.;
- Als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende wordt in zijn taak ondersteund door de Privacy Officer. Leidinggevendens hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

6.2 Overzicht 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. Het overzicht op de volgende pagina is een schematische weergave van deze verantwoordelijkheden en taken.

	Wie Rollen	Hoe Verantwoordelijkheid/taken	Wat Realiseren/vastleggen
Richtinggevend (Strategisch)	Bestuurder	• Eindverantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens. • Vastleggen en uitdragen van IBP-beleid. • Evalueren IBP-beleid op basis van rapportages. • Organisatie IBP inrichten.	• Informatiebeveiligings- en privacy beleid. • Reglement FG. • Privacyreglement. • Gedragscode medewerkers en leerlingen.
	Manager IBP	• Domeinverantwoordelijk voor uitvoering en aansturing IBP beleid en PDCA-cyclus. • Adviseert het Dir. Best. over IBP. • Voorbereiden uitvoering IBP-beleid, classificatie en risicoanalyse. • Hanteren IBP normen en wijze van toetsen. • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze. • Schrijven en beheren van maatregelen, processen, richtlijnen en procedures om de uitvoering te ondersteunen.	• Vormgeven van processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender. • Protocol beveiligingsincidenten en datalekken. • Verwerkersovereenkomsten. • Toestemming gebruik beeldmateriaal. • Opstellen informatie en documentatie richting leerlingen, ouders/verzorgers. • Sociale media reglement. • Gedragscode ict en internetgebruik. • Inrichten meldpunt beveiligingsincidenten.
Sturend (Tactisch)	Teamleider ICT	• Domeinverantwoordelijk voor uitvoering en aansturing ICT beleid en PDCA-cyclus. • Adviseert bestuurder over ICT en IBP. • Classificatie/risicoanalyse in samenwerking met Manager IBP/Privacy Officer • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuurder • 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.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister • Classificatie- en risicoanalyse documenten. • Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

	Functionaris voor de gegevensbescherming	• Toezicht op naleving privacy-wetgeving. • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens. • Afwikkeling klachten en incidenten.	• Overleg met bestuurder en met manager IBP
	Privacy Officer	• Toezicht op naleving privacy-wetgeving op schoolniveau. • Advisering over en uitwerking van privacyvraagstukken, IBP, werkprocessen, richtlijnen, bewustwording, et cetera. • Schakel en klankbord tussen de werkvloer en het beleid.	• Privacyreglement • Voorlichting privacy en stimuleren bewustwording • Procedure IBP-incident afhandeling Incidenten meldpunt datalekken • De werkgroep PO komt meerdere keren bijeen.
	Domeinverantwoordelijke/proceseigenaar waaronder ICT, HRM, financiën, facilitair, onderwijs, zorg, leerlingenadministratie	• Classificatie/risicoanalyse in samenwerking met manager IBP • Toegangsbeleid zowel fysiek als digitaal vaststellen. • Samen met facilitair beheer en ICT-beheer erop toezien dat het toegangsbeleid gehanteerd wordt. • Samen met facilitair beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister. • Classificatie- en risicoanalyse documenten. • Autorisatietabel/ toegangsmatrix voor de diverse informatiesystemen en netwerk. • Sleutel- en gebouwbeheer. • Melden incidenten.
Uitvoerend (Operationeel)	Systeem- en netwerkbeheerder	• Technisch aanspreekpunt voor informatiebeveiliging en privacy voor management en medewerkers.	• Melden incidenten.
	Functioneel en/of applicatie beheerder	• Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij de dagelijkse werkzaamheden.	• Melden incidenten.
	Medewerker	• Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij de dagelijkse werkzaamheden.	• Melden incidenten.
	Leidinggevende	• Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen tijdens de gesprekkencyclus, werkoverleggen, beoordelingen et cetera. • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen. • Voorbeeldgedrag. • Omgang met het leerlingvolgsysteem en leerlingendossiers. • Het delen van persoonsgegevens binnen en buiten de organisatie. • Naleven gedragscode. • Omgang met sociale media. • Bewustwording, mediawijs maken.

Bijlage 1: Uitwerkingen van mogelijke maatregelen

In deze staan een aantal uitwerkingen van organisatorische- en technische maatregelen. Deze bijlage dient ter illustratie en is niet uitputtend.

Beveiliging van personeel

- Medewerkers overleggen voor indiensttreding een Verklaring Omtrent het Gedrag (VOG). De VOG wordt indien nodig herhaald tijdens het dienstverband.
- Een medewerker krijgt autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens op basis van de rol die hij vervult, bijvoorbeeld docent, mentor, leidinggevende.
- Medewerkers worden geschoold in het zorgvuldig omgaan met persoonsgegevens, door middel van een basistraining.
- In de gesprekkencyclus en andere overleggen wordt aandacht geschonken aan informatieveiligheid en privacy.
- Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in de cao-vo.
- Bij beëindiging van het dienstverband worden alle bedrijfsmiddelen geretourneerd, dit betreft o.a. de in bruikleen gestelde devices en sleutels van het gebouw. De toegang tot ict-middelen en informatiesystemen wordt na beëindiging van het dienstverband automatisch geblokkeerd.

Fysieke beveiliging en beveiliging van de omgeving

- De toegang tot de verschillende gebouwen, gebouwdelen, lokalen en ruimten is vastgesteld met een sleutelbeheerplan. De uitgifte van sleutels wordt geregistreerd.
- Op meerdere plekken in en rondom het gebouw wordt gebruik gemaakt van cameratoezicht.
- De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden is voorbehouden aan bevoegd personeel.
- Reserveapparatuur en back-ups zijn gescheiden op twee locaties, om de gevolgen van een calamiteit te minimaliseren.
- Gegevens en programmatuur worden verwijderd of veilig overschreven, voordat de apparatuur wordt afgevoerd.

Mobiele apparatuur

- Beveiligingsmaatregelen hebben betrekking op zowel door de school verstrekte middelen als privé-apparatuur. Op privé-apparatuur binnen het wifinetwerk is de school bevoegd om beveiligingsinstellingen af te dwingen. Bijvoorbeeld: controle op wachtwoord, encryptie, aanwezigheid van malware, et cetera.
- Op verzoek dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan, denk bijvoorbeeld aan 'mobile device management software'. De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming en beveiliging van het schoolnetwerk.
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privémiddelen en privébestanden. Dit betreft enkel devices van de school en/of programma's en bestanden binnen een door school aangewezen bestandsstructuur.

Controle

- Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet in het geding komt.
- Het gebruik van ICT-middelen wordt gemonitord ten behoeve van een tijdige aanpassing van de beschikbare capaciteit aan de vraag.

- Het gebruik van informatiesystemen, waaronder ook uitzonderingen en beveiligingsincidenten, wordt vastgelegd in logbestanden. De volgende zaken kunnen in de logs worden opgenomen:
 - type gebeurtenis (zoals back-up/restore, reset wachtwoord, betreden ruimte);
 - (poging tot) ongeautoriseerde toegang;
 - systeemwaarschuwingen;
 - (poging tot) wijziging van de beveiligingsinstellingen.
- Een logregel bevat minimaal:
 - een tot een natuurlijk persoon herleidbare gebruikersnaam of ID;
 - de gebeurtenis;
 - waar mogelijk de identiteit van het werkstation of de locatie;
 - het object waarop de handeling werd uitgevoerd;
 - het resultaat van de handeling;
 - de datum en het tijdstip van de gebeurtenis.
 - In een logregel worden alleen de voor de rapportage noodzakelijke gegevens opgeslagen.
 - Er worden maatregelen getroffen om te verzekeren dat gegevens over logging beschikbaar blijven en niet gewijzigd kunnen worden door een gebruiker. De bewaartermijnen zijn in overeenstemming met wettelijke eisen.

Beveiliging van apparatuur en informatie

- Er is een scheiding tussen beheertaken en gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken wanneer ingelogd als gebruiker.
- Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en kunnen pas daarna geïmplementeerd worden. In nieuwe situaties met verstrekking van gevolgen voor de privacy en het verwerken van (bijzondere) persoonsgegevens dient een DPIA uitgevoerd te worden.
- Vertrouwelijke data mag niet worden gebruikt in een testomgeving tenzij de gegevens zijn geanonimiseerd. Indien het toch noodzakelijk is om data uit productie te gebruiken, is er vooraf toestemming van de teamleider ict vereist en dienen er afspraken te worden gemaakt om data te vernietigen na ontwikkelen en testen.
- Versleuteling van gegevens vindt plaats conform 'best practices' (de stand der techniek), waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn. Gegevens op papier worden beschermd door een deugdelijke opslag.
- Op verschillende niveaus binnen de ICT-infrastructuur (netwerkcomponenten, firewall, pc's) wordt antivirussoftware toegepast.
- E-mail met persoonsgegevens wordt vertrouwelijk verzonden.
- Apparatuur die is verbonden met het netwerk van de school moet kunnen worden geïdentificeerd.
- Documenten, opslagmedia, in- en uitvoergegevens en systeemdokumentatie worden beschermd tegen onbevoegde verwerking op basis van rollen en autorisaties.
- Alle informatie die wordt geplaatst op de website van de school, wordt beschermd tegen onbevoegde wijziging op basis van rollen en autorisaties. Op de publieke website wordt alleen openbare informatie gepubliceerd.
- Groepen gebruikers en informatiesystemen worden op het netwerk gescheiden zodat de kans op onbevoegde toegang tot gegevens verder wordt verkleind. Er is sprake van segmentering van netwerkzones.

Back-up en recovery

- ICT-beheer maakt back-ups van alle essentiële bedrijfsgegevens en programmatuur zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd.
- De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering.
- Data en back-up worden gescheiden (tenminste 2 verschillende gebouwdelen) bewaard.

- De back-up en herstelprocedures worden regelmatig (tenminste eenmaal per jaar) getest om de betrouwbaarheid ervan vast te stellen.

Beheer van de dienstverlening door een derde partij

Bij externe hosting van data en/of services blijft de school eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop.

- Beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening worden vastgelegd in een (verwerkers)overeenkomst of SLA. De (verwerkers)overeenkomst of SLA worden in beginsel getekend door de bestuurder of het hoofd ICT.
- Bewerksovereenkomsten voor digitale leermiddelen volgen zo veel mogelijk de actuele versies van het onderwijsconvenant voor verwerkersovereenkomsten.
- In een (verwerkers)overkomst of SLA wordt aandacht besteed aan informatiebeveiliging.

Autorisatie en authenticatie

- Autorisaties worden toegekend via functie(s) en organisatieonderdelen. Autorisatie is rol gebaseerd.
- Wachtwoorden worden voor een beperkte periode toegekend en dienen aan een aantal technische eisen te voldoen. Deze eisen worden afgedwongen door het systeem. Voor medewerkers met speciale bevoegdheden, zoals systeem en functioneel beheerders) gelden strengere eisen.
- De technische eisen voor wachtwoorden zijn uitgewerkt in een wachtwoordenbeleid.
- Elke gebruiker is verantwoordelijk voor het geheim houden van zijn wachtwoord.
- Authenticatiemiddelen zoals wachtwoorden worden beschermd tegen inzage en wijziging door onbevoegden tijdens transport en opslag (bijvoorbeeld door middel van hashing, encryptie).
- Bij toegang tot belangrijke informatiesystemen is tweefactorautorisatie vereist.

Mobiel en thuiswerken

- Voor werken op afstand is een thuiswerkomgeving beschikbaar, toegang wordt verleend op basis van tweefactorauthenticatie.
- Onbeheerde apparatuur kan gebruik maken van het draadloze netwerk (wifi) middels een private pre-shared key, dan wel een voucher met beperkte geldigheid. Het draadloze netwerk is logisch gescheiden van het bedrijfsnetwerk.
- Het fysieke (bekabelde) netwerk is niet toegankelijk voor onbeheerde apparatuur.

Melding en registratie van incidenten

- Elke medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct te melden bij de direct leidinggevende, Privacy Officer of de FG.
- Meldingen worden geregistreerd in een incidentenregister. Voor afhandeling geldt een procedure zoals omschreven in het beleidsplan datalekken.