

Beleidsnotitie Informatiebeveiliging en privacy (IBP)

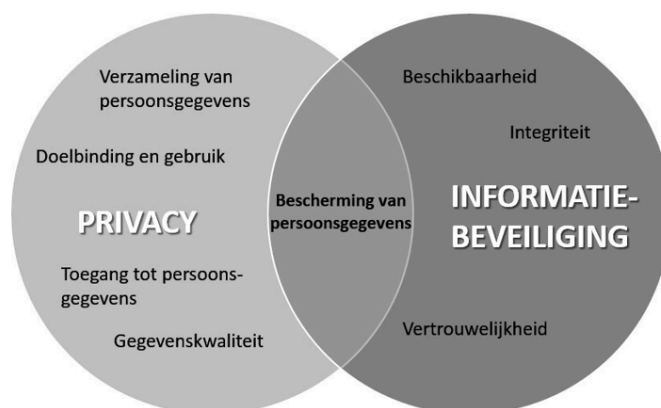
Verantwoordelijke	Naam: college van bestuur
	Vastgesteld in: november 2025 Geëvalueerd in:

Inleiding

In dit document staat ons IBP-beleid omschreven. Het is een dynamisch document, dat gaandeweg het werken aan IBP-normenkader verder wordt aangepast en aangevuld, met tekst of linkjes naar separate beleidsdocumenten. Aan dit beleid worden kwaliteitskaarten gekoppeld waarin procedures en processen zijn beschreven. Dit document begint met het omschrijven van het belang van informatiebeveiliging en privacy. Daarna volgt het doel en de reikwijdte hiervan. Vervolgens beschrijven we de uitgangspunten van ons beleid en een uitwerking daarvan. Tot slot verwijzen we naar hoe de taken en verantwoordelijkheden voor dit beleid zijn verdeeld.

1. Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid digitale informatie die gebruikt wordt neemt toe, door onder andere ontwikkelingen als gepersonaliseerd leren met ICT, leerlingadministratiesystemen en digitale communicatie. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt bovendien 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.



Dit Informatiebeveiligings- en privacybeleid (IBP-beleid) is opgesteld door Talent Primair en geldt voor alle onder het bevoegd gezag staande scholen voor primair onderwijs.

Strategische context en urgentie

Digitale afhankelijkheid in het onderwijs maakt informatiebeveiliging cruciaal. Ransomware, datalekken of verstoringen kunnen het onderwijsproces ontwrichten, leiden tot reputatieschade en bestuurlijke aansprakelijkheid.

De wetgeving (zoals AVG en NIS2), inspectiekaders en governancecodes vereisen aantoonbare borging. Talent Primair positioneert IBP daarom als integraal onderdeel van onderwijskwaliteit en goed bestuur. Daarbij is een juiste balans nodig tussen risicoacceptatie, beheersmaatregelen en investeringen (FTE, tooling, bewustwording).

Talent Primair sluit voor de verdere concretisering van de strategische borging van IBP aan bij het toetsingskader voor informatiebeveiliging en privacy, evenals bij de ontwikkelde referentiedocumenten die

richtinggevend zijn voor de sector funderend onderwijs. Deze kaders worden gehanteerd als aanvullend fundament voor de inrichting van governance, processen en techniek. Door deze referenties expliciet te hanteren kan Talent Primair de samenhang tussen interne ambities en externe toezichtskaders beter aantoonbaar maken.

2. Toelichting informatiebeveiliging en privacy

2.1. Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een aantal 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 IPB-beleid, vormt de basis om informatiebeveiliging en privacy binnen Talent Primair te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3. Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy hebben de volgende doelen:

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

Het informatiebeveiligings- en privacybeleid (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 (onder andere medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en Talent Primair voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen Talent Primair geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers, vrijwilligers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Talent Primair. 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. (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 Talent Primair 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 Talent Primair 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.
 - De nadere invulling van dit beleid is gebaseerd op drie samenhangende pijlers:
 - Governance (G01 – G07): de inrichting van beleid, strategie, eigenaarschap, risicomanagement en toetsing.
 - Processen (P08 – P14): de borging van HR, ITIL-processen, data management, identity & access management, security baselines, business continuity en leveranciersbeheer.
 - Techniek (T15 – T21): de inzet van technische maatregelen en standaarden ter versterking van de weerbaarheid.
 - Deze pijlers vormen gezamenlijk de kapstok waarlangs de concrete invulling van maatregelen en controles wordt uitgewerkt. De indeling maakt het mogelijk om eenduidig te sturen, te toetsen en te rapporteren.

4. Beleid – Hoe doen we dat?

Talent Primair hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken, waarbij wordt voldaan aan de wet- en regelgeving:

Verantwoordelijkheidsverdeling

- Het bestuur van Talent Primair neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
- Talent Primair 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.
- Binnen Talent Primair is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van alle medewerkers. Dit omvat met name het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie als ook van papieren documenten.

- Talent Primair 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. Talent Primair heeft een gedragscode geformuleerd die nieuwe medewerkers moeten ondertekenen.
- Talent Primair is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers worden geïnformeerd over de regelgeving rondom het gebruik van informatie.

Specifieke doelen

- Bij Talent Primair is het belangrijk dat de verwerking van persoonsgegevens gekoppeld is aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Talent Primair 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.

Informereren betrokkenen

- Talent Primair streeft ernaar alle betrokkenen helder en actief te informeren over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Daarbij streven Talent Primair ernaar alle betrokkenen te wijzen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.

Vastleggen verwerkingen en monitoring

- Informatiebeveiliging en privacy is bij Talent Primair een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Talent Primair formuleert een procedure voor verwerkingen van persoonsgegevens in een up-to-date verwerkingsregister voor de verantwoordings- en documentatieplicht.
- Talent Primair gebruikt een systeem om beveiligingsincidenten vast te leggen en heeft een procedure voor het afhandelen en melden van datalekken bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

Werken met systemen en leveranciers

- Talent Primair maakt risico-analyses met beheersmaatregelen. Er wordt gezocht naar een balans tussen geconstateerde risico's en investeringen om de benodigde maatregelen te mitigeren.
- Talent Primair sluit met leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfs-applicaties) 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.
- Talent Primair heeft bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf oog voor de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig juiste maatregelen kunnen worden genomen.
- Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt, wordt nagegaan of de informatie technisch voldoende beveiligd is.

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 primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO

- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Talent Primair hanteert aanvullende toetsingskaders en referenties die in de sector funderend onderwijs zijn ontwikkeld. Dit betreft het Normenkader Informatiebeveiliging voor het Funderend Onderwijs en opgestelde referentiedocumenten, waaronder de thema's governance, processen en technische weerbaarheid. Deze documenten worden als leidraad gebruikt bij het handelen.

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. Talent Primair stimuleert scholen om volgens deze vuistregels te werken.

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 moet de hoeveelheid en het soort gegevens beperkt zijn: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding 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:** scholen leggen 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 kan gevraagd en ongevraagd plaatsvinden. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen aangeven bezwaar te hebben tegen het gebruik van hun gegevens.
5. **Data-integriteit:** de te verwerken persoonsgegevens zijn juist en actueel.

5.3. Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid.

Daarnaast worden verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een verwerkingsregister.

5.4. Voorlichting en bewustzijn

Beleid en maatregelen staan niet op zichzelf 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 regelmatig aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn regelmatig terugkerende momenten voor bewustwording voor medewerkers, leerlingen en gasten, volgens onze huidige manier van werken. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van onder andere bovenschoolse medewerkers waaronder de interne privacy officer, alsook de directeuren en i-coaches.

5.5. Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom is het belangrijk dat alle gegevens en informatiesystemen waarop dit beleid van toepassing is, worden 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.

Talent Primair kan het ROSA-model (Risico- en Objectclassificatie Systeem Architectuur) gebruiken als hulpmiddel voor het classificeren van informatie. De classificatie op basis van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) bepaalt dan het niveau van maatregelen.

De classificatie kan als uitgangspunt gebruikt worden voor risicoanalyse en, waar wettelijk nodig, privacy toetsen (Data Protection Impact Assessment - DPIA's).

Talent Primair stelt jaarlijks een risico-analyse op met beheersmaatregelen.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, is aandacht voor 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 medewerkers die een beveiligingsincident of datalek vermoeden, dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in de kwaliteitskaart GB.01 Datalek detectie-, meld- en afhandelingsproces.

5.7. Planning en controle

Talent Primair streeft naar inbedding van het IBP-beleid in de planning en controlcyclus van Talent Primair en daarmee ook naar evaluatie van dit beleid. De bovenschoolse ict'er en de interne privacy-officer bespreken deze evaluatie jaarlijks met het bestuur en gaan na waar het IBP-beleid aanpassing behoeft.



en
dit

5.8. Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Dit is een taak van schooldirecteuren en het bestuursbureau. Vanuit het bestuursbureau (o.a. door de bovenschoolse ict'er en de interne privacy officer), door i-coaches en schooldirecteuren wordt actief aandacht besteed aan IBP. Mogelijke momenten daartoe zijn op het moment van aanstelling, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode, met periodieke bewustwordingsacties, et cetera. Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol.

Talent Primair heeft de rol van Functionaris voor Gegevensbescherming (FG) extern belegd. De externe FG vervult een wettelijk omschreven en onafhankelijke toezichthoudende functie en opereert op basis van een door het bestuur vastgesteld reglement. De FG wordt tijdig betrokken bij alle aangelegenheden waarbij persoonsgegevens worden verwerkt.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Talent Primair de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.9. Logging en monitoring

Logging en monitoring zijn essentieel voor toezicht op informatiebeveiliging. Het is belangrijk dat Talent Primair het volgende registreert:

- Pogingen tot inloggen en systeemtoegang (geslaagd/mislukt);
- Activiteit op kritieke systemen (mutaties, downloads, systeemwijzigingen);
- Beveiligingsgebeurtenissen in SIEM-systemen;

Het is goed om loggegevens minimaal 180 dagen te bewaren, en analyses van logs steekproefsgewijs plaats te laten vinden.

5.10 DPIA en privacy by design

Talent Primair voert bij nieuwe systemen of ingrijpende wijzigingen waar nodig een DPIA (Data Protection Impact Assessment) uit. Hiervoor is een kwaliteitskaart DPIA gemaakt. Dit proces identificeert risico's voor betrokkenen en borgt dat mitigerende maatregelen tijdig worden getroffen. Privacy by design en by default zijn uitgangspunt bij inrichting van systemen of processen die persoonsgegevens verwerken.

6. Organisatie - Wie doet wat?

De taken, verantwoordelijkheden en bevoegdheden (TVB) staan nader gespecificeerd in G04 - Eigenaarschap en verantwoordelijkheden.