# Informatiebeveiligings- en privacybeleid

## CVO Baarn/Soest

stichting voor Christelijk Voortgezet Onderwijs Baarn/Soest

| Versie | Datum | type | Akkoord | Naam |
|---|---|---|---|---|
| 0 | Sept 2021 | draft | Privacy Team | IBP CVO BaarnSoest - draft 210716 |
| 0.1 | Sept 2021 | voorstel | MT | IBP CVO BaarnSoest – voorstel 210909 |
| 0.2 | Okt 2021 | voorstel | MR | IBP CVO BaarnSoest – voorstel 210909 |
| 1.0 | 19 januari 2022 | definitief | GMR | IBP CVO Baarn Soest – versie 1.0 |

Instemming versie 1.0

# Inhoudsopgave

# 1 Inleiding

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. Deze afhankelijkheid van ict en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

# 2 Toelichting informatiebeveiliging en privacy

## 2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.

1. Informatiebeveiliging richt zich op de volgende aspecten:
   Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
2. Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
3. 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. 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. Deze regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

### 2.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen de stichting voor Christelijk Voortgezet Onderwijs Baarn/Soest (hierna te noemen: CVO) te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

# 3 Doel en reikwijdte

## 3.1 Doel

Dit beleid heeft de volgende doelen:

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

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

## 3.2 Reikwijdte

1. Het IBP-beleid binnen het CVO geldt voor alle medewerkers, tijdelijk personeel, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties.
2. Onder dit beleid vallen ook alle *devices* van waar geautoriseerde toegang tot het wifi-netwerk van een van beide scholen verkregen kan worden.
3. Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen het CVO waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan het CVO persoonsgegevens verwerkt.
4. Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het CVO.
5. Het IBP-beleid geldt voor de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van het CVO 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.
6. Het IBP-beleid heeft binnen het CVO raakvlakken met:
    1. Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.
    2. Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
    3. IT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT.
    4. Medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers
    5. Professionaliseringsbeleid met als aandachtspunt de digitaal-didactische vaardigheden en mediawijsheid onderwijzend personeel.
    6. Onderwijsbeleid – met als aandachtspunten:
        1. Beleid inzake aanschaf en gebruik van digitale leeromgeving, digitale leermiddelen
        2. Toets- en examenbeleid, voorkomen van fraude
        3. Doorstroomgegevens uitwisselen met basisscholen en vervolgonderwijs.

# 4 Beleid – uitgangspunten

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

1. Het schoolbestuur van het CVO 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.

2. Binnen het CVO 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. Binnen het CVO opereert een privacyteam met als doel om het bestuur en de organisatie te adviseren en waar nodig te ondersteunen bij de uitvoering van dit IBP.

4. Het CVO voldoet aan alle relevante wet- en regelgeving.

5. Bij het CVO 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 het CVO om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.

6. We stellen informatie beschikbaar daar waar nodig voor het doel waar het voor gebruikt wordt (rollen- en rechtenstructuur).

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

8. Het CVO legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Het CVO voldoet hiermee aan de documentatieplicht.

9. Het CVO is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.

10. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen. Het CVO volgt daarbij de actuele adviezen van sectororganisaties ten aanzien van informatiebeveiliging.

11. Het CVO maakt met partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over de informatiebeveiliging en privacy (middels een verwerkersovereenkomst of waar nodig een passende afspraak met verwerkingsverantwoordelijke).

12. Informatiebeveiliging en privacy is bij het CVO een continu proces, waarbij regelmatig wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

13. Het CVO 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. Het CVO 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.

15. Het CVO zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol (handboek datalek CVO Baarn/Soest) afhandelen en indien nodig melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

## 4.1 Relevante wet- en regelgeving

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

1. Wet voortgezet onderwijs en/of Wet op de expertisecentra
2. Wet goed onderwijs en goed bestuur VO
3. Wet onderwijstoezicht
4. Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
5. Archiefwet
6. Leerplichtwet
7. Auteurswet
8. Wetboek van Strafrecht
9. CAO VO
10. Wet Passend Onderwijs
11. Examens en toetsing (gepubliceerd op Examenblad.nl)

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) wordt als richtinggevend naslagwerk ingezet 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.

## 4.2 Basisregels bij het omgaan met persoonsgegevens

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

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.

Grondslag: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene of gerechtvaardigd belang.

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

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.

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

# 5 Uitwerking van het beleid – Wat doen we?

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

## 5.1 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen.

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

## 5.2 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.
Op de AFAS-*Insight* website van het CVO staan alle actuele beleidsdocumenten geplaatst. Daarnaast zullen er (online) trainingen worden verzorgd voor de medewerkers en wordt periodiek een (mid)weekbericht verspreid.

## 5.3 Risicoanalyse

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

## 5.4 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.
Alle (beveiligings-)incidenten kunnen worden gemeld volgens het protocol ‘handboek datalek CVO Baarn/Soest’ bij fg@cvobaarnsoest.nl.

## 5.5 Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur en jaarlijks getoetst. Hierbij wordt rekening gehouden met:

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

Daarnaast kent het CVO een IBP-jaarplanning waarin de planning en control cyclus voor informatiebeveiliging en privacy is opgenomen. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

Op termijn wordt het IPB middels externe audits getoetst.

## 5.6 Naleving

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 het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

Het CVO wordt beoordeeld op de naleving van de AVG door de FG. De laatste beoordeling vond plaats in november 2020.

# 6 Organisatie - Wie doet wat?

## 6.1 Rollen en verantwoordelijkheden

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij het CVO voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

In deze paragraaf wordt beschreven hoe IBP op drie niveaus binnen het CVO wordt georganiseerd. Die drie niveaus zijn onder te verdelen in

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

Vervolgens wordt in een schematisch overzicht weergegeven welke verantwoordelijkheden en taken bij welke rollen horen bij het CVO.

## 6.2 Richtinggevende rol (strategisch)

Het bestuur is eindverantwoordelijk voor het IBP-beleid en stelt – in overleg met de directies van beide scholen– 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.

## 6.3 Sturende rol (tactisch) / Uitvoerende rol (operationeel)

### 6.3.1 Privacyteam (uitvoerend en adviserend richting Bestuur)

De ondersteuning en aansturing van IBP is bij het CVO belegd bij het privacyteam als onderdeel van de ‘gewone ’bedrijfsvoering. Het privacyteam bestaat uit de Privacy Officer (PO), de leidinggevende van systeembeheer/ICT, teamleider Waldheim-mavo, plaatsvervangend rector Griftland College en de functionaris voor gegevensbescherming.

- Handelt bij incidenten op het gebied van IBP in overleg met de fg.

### 6.3.2 Privacy-werkgroep (uitvoerend en adviserend richting Bestuur)

De privacy-werkgroep die aan het privacyteam is verbonden adviseert en ondersteunt t.a.v. het IBP-beleid en de (praktische) invulling hiervan. De privacy-werkgroep bestaat uit de applicatiebeheerders, systeembeheerders/ICT en de medewerker PR.

### 6.3.3 Privacy Officer (PO)

De PO is een rol op sturend en uitvoerend niveau. De PO:

- Geeft terugkoppeling en advies aan de eindverantwoordelijke (de bestuurder);

- Vertaalt (of laat vertalen) het beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling en houdt deze up-to-date;
- Bewaakt de uniformiteit binnen het CVO;
- Is het aanspreekpunt voor incidenten op het gebied van informatiebeveiliging en privacy;
- Initieert IBP-activiteiten en stelt de jaarplanning op.
- Is vraagbaak op het gebied van IBP

De rol van PO wordt binnen het CVO ingevuld door hoofd Centrale administratie / Controller.

### 6.3.4 De leidinggevende systeembeheer/ICT

De werkzaamheden van systeembeheer/ICT bestrijken een breed gebied van ICT in onderwijs en bedrijfsvoering; informatiebeveiliging en privacy is één van de aandachtspunten. De leidinggevende ICT is onderdeel van het privacyteam.
De afdeling ICT heeft een signalerende en adviserende rol met betrekking tot de naleving van het informatiebeveiligings- en privacybeleid ten behoeve van het privacyteam.

### 6.3.5 Functionaris voor Gegevensbescherming

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

Wij hebben een externe Functionaris voor de Gegevensbescherming (FG) aangesteld, te weten Pim van Buuren.

Contactgegevens: FG@cvobaarnsoest.nl

## 6.4 Uitvoerende rol (operationeel): proceseigenaren

Binnen de school zijn er verschillende processen, zoals het primaire onderwijsproces, (leerlingen)administratie, ICT, personeel, facilitaire- en financiële zaken etc. Op elk van deze processen is een proceseigenaar verantwoordelijk om – binnen de kaders van het IBP-beleid – te bepalen op welke wijze IBP wordt uitgewerkt in richtlijnen, procedures en instructies.

### 6.4.1 Leidinggevenden (teamleiders, hoofd administratie, hoofd facilitair, etc.)

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:
1. er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;

2. toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
3. periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
4. als aanspreekpunt beschikbaar te zijn voor alle IBP-onderwerpen waar het personeel mee te maken heeft.

Op het gebied van informatiebeveiliging en privacy hebben leidinggevenden een belangrijke voorbeeldfunctie voor hun medewerkers.

### 6.4.2 Medewerkers OP en OOP

Elke medewerker heeft verantwoordelijkheden met betrekking tot informatiebeveiliging in zijn of haar dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. de gedragscode en het protocol ICT.
Medewerkers worden gestimuleerd om actief betrokken te zijn bij informatiebeveiliging en actief kennis te nemen van de beschikbare documentatie (beschikbaar via AFAS Insight).
Medewerkers maken melding van datalekken en veiligheidsincidenten, doen verbetervoorstellen etc.

## Overzicht rollen, verantwoordelijkheden en taken

| Niveau | Wie<br>Rollen | Hoe Verantwoordelijkheid / taken | Wat Realiseren / vastleggen |
|---|---|---|---|
| Richtinggevend (strategisch) | Bestuurder | Eindverantwoordelijk IBP-beleidsvorming, vastlegging en het uitdragen ervan<br><br>Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens<br><br>Evalueren toepassing en werking IBP-beleid op basis van rapportages<br><br>Aanstellen FG-er | Informatiebeveiligings- en privacybeleid vaststellen<br>Inrichten IBP organisatie<br><br>Basismaatregelen nemen<br><br>Reglement FG vaststellen<br>Privacyreglement vaststellen |
| Sturend / uitvoerend | Privacyteam<br>Bestaande uit:<br>onderstaande rollen | IBP-planning en controle<br><br>Adviseert Bestuur over IBP Hanteren IBP normen en wijze van toetsen<br><br>Evalueren IBP-beleid en maatregelen<br><br>Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze<br><br>is het aanspreekpunt voor incidenten op het gebied van informatiebeveiliging en privacy; | Opstellen jaarplanning.<br><br>Actualiseren van processen, richtlijnen en procedures .<br><br>Verwerkingsregister opstellen en actueel houden.<br><br>Afwikkelen klachten en incidenten |
| | Privacy Officer | geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur);<br><br>vertaalt het beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling en houdt deze up-to-date;<br><br>bewaakt de uniformiteit binnen het CVO;<br><br>initieert IBP-activiteiten en stelt de jaarplanning op.<br><br>handelt bij incidenten op het gebied van IBP in overleg met de fg.<br><br>is vraagbaak op het gebied van IBP<br><br>Beheer en inrichting cameratoezicht Etc. | Incidentafhandeling (registreren en evalueren).<br><br>vertaalt het beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling.<br><br>Neemt deel aan regionaal netwerk IBP<br><br>Aanspreekpunt binnen CVO<br><br>Agenderen stukken etc. in schoolleiding en GMR<br><br>Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst);<br><br>verwerkersovereenkomsten opstellen en registeren in overleg met fg<br><br>Risico-analyse (DPIA) |

| | | | |
|---|---|---|---|
| | Afdelingsleider Waldheim-Mavo en Plaatsveravngend rector Griftland College | Signaleren voortgang en dagelijkse gang van zaken ten aanzien van het IPB. Proceseigenaar implementatie van het IPB.<br><br>Er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.<br><br>De toegangsrechten van gebruikers regelmatig beoordelen en controleren. | Frequente input vanuit de scholen in het privacyteam.<br><br>Regelmatige evaluatie en bijstelling van het IPB ter goedkeuring van het bestuur.<br><br>Aanspreekpunt binnen CVO |
| | Privacy-werkgroep | Adviseert en ondersteunt het IBP. | de (praktische) invulling hiervan |
| | Leidinggevende ICT | Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur | Technisch aanspreekpunt voor IBP.<br><br>Incidentafhandeling op technisch gebied (met afdeling ICT) |
| | Proceseigenaren | Signaleren van privacyrisico's<br><br>Naleving IBP in de primaire processen | Diverse aanvullende werkwijzen.<br><br>Rapportage van risico's (en naleving) bij voorkeur in de vorm van good practices. |
| | Functionaris voor Gegevensbescherming | Toezicht op naleving privacy wetgeving<br><br>Aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens Afwikkeling klachten en incidenten<br>Zie de functieomschrijving zoals opgesteld door de VO raad | Regelmatige Privacyrapportages<br><br>Is aangesteld door CVO. |
| | Medewerker | Verantwoordelijk omgaan met IBP bij de dagelijkse werkzaamheden.<br><br>Pro-actieve houding om informatie, documentatie, regelingen etc. t.a.v. IPB tot zich te nemen. | Naleving IBP bij werkzaamheden voor het CVO (op school en thuis). |

| | | | |
|---|---|---|---|
| | Schoolleiding<br>Teamleiders<br>Hoofden afdelingen | Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP beleid en de consequenties ervan.<br><br>Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers.<br><br>Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid.<br><br>Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen | Communiceren, informeren en toezien op naleving van o.a.:<br>IBP in het algemeen<br>Regels passend onderwijs<br>Hoe omgaan met leerling dossiers<br>Wie mogen wat zien<br>Gedragscode Omgaan met sociale media<br>Mediawijs maken |