Informatiebeveiligings- en Privacybeleid

Versie	Status	Datum	Naam	Omschrijving
1.0	Beoordeeld FG Instemming GMR Vastgesteld CvB	december 2022 11 april 2023 12 april 2023	PRA	Def. versie
1.1		1 februari 2024	PRA	Aanpassing nieuwe FG

Inhoudsopgave

1. Inleiding

In het onderwijs worden veel gegevens gebruikt en gedeeld. Deze gegevens verwijzen in de meeste gevallen naar personen. Het gaat hierbij onder meer over gegevens van leerlingen, ouders en docenten. We noemen deze gegevens persoonsgegevens.

In de Europese Unie, en dus ook in Nederland, geldt de Algemene Verordening Gegevensbescherming (AVG), ook wel de Privacywet genoemd. Op de uitvoering van deze wet wordt toezicht gehouden door de Autoriteit Persoonsgegevens (AP). Deze wetgeving houdt in dat alle bedrijven en organisaties aan de AVG moeten voldoen en hiervoor moeten zorgen voor bescherming en beveiliging van persoonsgegevens.

Het College van Bestuur (CvB) van de Pontis Onderwijsgroep, met de scholen Regius College en Trinitas College, is verantwoordelijk voor de ontwikkeling en uitvoering van het Informatiebeveiliging en privacy beleid (IBP). Met dit IBP-beleid wordt aan alle betrokkenen inzicht gegeven in de eisen die worden gesteld aan het verwerken van persoonsgegevens en hoe hiermee de privacy wordt gewaarborgd.

2. Informatiebeveiliging en privacy

2.1. (Toelichting) informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

- Beschikbaarheid: de informatie is beschikbaar op het moment, de tijd, het apparaat en de locatie die je wilt als organisatie.
- Integriteit: de informatie die je gebruikt is volledig, actueel en geeft een juist beeld.
- Vertrouwelijkheid: alleen de juiste mensen – die daartoe bevoegd zijn – hebben toegang tot de informatie.

Na het proces van vaststellen, wordt de uitvoering en het toezicht op de uitvoering geregeld. Hiervoor zijn functionarissen aangesteld die verantwoordelijk zijn voor het deel van de uitvoering waarmee zij belast zijn. Uiteindelijk zijn het College van Bestuur en de schooldirecties verantwoordelijk voor de kwaliteit en de veiligheid van de binnen de organisatie gebruikte informatiesystemen.

2.2. (Toelichting) privacy

Ieder mens heeft recht op privacy. Dit ligt in de wet verankerd en betekent dat ieder persoon in de gelegenheid gesteld moet worden om informatie over zichzelf af te schermen, dat wil zeggen dat een persoon zelf kan bepalen welke informatie hij deelt met anderen.

Om deel te kunnen nemen aan het onderwijs is het nodig dat bepaalde informatie van leerlingen, ouders en medewerkers wel bekend is bij de schoolorganisatie. Belangrijk hierbij is dat zij er op kunnen vertrouwen dat de informatie die wordt gevraagd en gebruikt door de schoolorganisatie (wettelijk) noodzakelijk is en goed beschermd wordt. In de privacy regelgeving wordt nadrukkelijk bepaald welke persoonsgegevens verwerkt mogen worden.

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

Om privacy van personen te kunnen waarborgen, is een goed systeem van informatiebeveiliging van persoonsgegevens nodig. De beleidsterreinen privacy en informatiebeveiliging van persoonsgegevens zijn zo vervlochten met elkaar dat ze samen het IBP-beleidsterrein vormen. Binnen dit terrein zorgen bestuur en scholen van de Pontis Onderwijsgroep voor verdere vormgeving en uitvoering van het IBP-beleid.

3. Doel en reikwijdte

3.1. Doel

Dit beleid heeft de volgende doelen:

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

Dit 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 betrokkenen wordt gerespecteerd en voldaan wordt aan relevante wet- en regelgeving.

3.2. Reikwijdte

- Het IBP-beleid binnen de Pontis Onderwijsgroep geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties. 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 hiervoor genoemde betrokkenen binnen de Pontis Onderwijsgroep, alsmede overige betrokkenen waarvan de Pontis Onderwijsgroep persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van de Pontis Onderwijsgroep.
- Het IBP-beleid geldt voor de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van persoonsgegevens, de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen en voor de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin opgenomen te worden.

3.2.1. Raakvlakken met andere beleidsterreinen

Het IBP-beleid binnen de Pontis Onderwijsgroep heeft 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.
- Medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers.
- Professionaliseringsbeleid, met als aandachtspunt de digitaal-didactische vaardigheden en mediawijsheid onderwijzend personeel.

- Onderwijsbeleid, met als aandachtspunten beleid inzake aanschaf en gebruik van digitale leeromgeving en digitale leermiddelen; toets- en examenbeleid en voorkomen van fraude; doorstroomgegevens uitwisselen met basisscholen en vervolgonderwijs.

4. Uitgangspunten

4.1. Beleidsuitgangspunten

De Pontis Onderwijsgroep hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het bestuur neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt binnen de organisatie. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
2. Het bestuur zorgt voor de correcte uitvoering van de relevante wet- en regelgeving.
3. De verwerking van persoonsgegevens is altijd gekoppeld aan een specifiek doel en gebaseerd op wettelijke grondslagen. Er vindt een goede belangenafweging plaats tussen het belang van de Pontis Onderwijsgroep om op correcte wijze persoonsgegevens te verwerken en het belang van betrokkene om zijn recht op privacy uit te oefenen. Bij alle verwerkingen van persoonsgegevens waarbij toestemming van betrokkenen noodzakelijk is, kunnen betrokkenen op elk moment hun toestemming herzien.

   ‘Indien er sprake is van verdere (secundaire) verwerking van persoonsgegevens (bijvoorbeeld voor het doel van (wetenschappelijk) onderzoek), dient te worden nagegaan of deze secundaire verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens oorspronkelijk verzameld werden. Betrokkenen dienen omtrent deze verdere (secundaire) verwerking van hun persoonsgegevens geïnformeerd te worden’.

4. Alle betrokkenen zullen correct, dat wil zeggen duidelijk en op tijd, worden geïnformeerd over de verwerking van hun persoonsgegevens. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
5. Alle verwerkingen van persoonsgegevens worden vastgelegd in een dataregister en worden up-to-date gehouden worden. De Pontis Onderwijsgroep voldoet hiermee aan de documentatieplicht.
6. Binnen de Pontis Onderwijsgroep is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
7. De Pontis Onderwijsgroep is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.
8. Er is een balans tussen de risico’s die we willen afdekken, de benodigde investeringen en de te nemen maatregelen.
9. Door middel van een verwerkersovereenkomst worden er met partijen waarmee persoonsgegevens worden uitgewisseld over de informatiebeveiliging en privacy concrete afspraken gemaakt.
10. Persoonsgegevens worden door Pontis Onderwijsgroep of haar verwerkers in principe niet buiten de EU/EER verwerkt. Indien dit het geval is, dan dragen wij er zorg voor dat de persoonsgegevens adequaat worden beschermd.
11. Informatiebeveiliging en privacy is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen wordt vóóraf gekeken naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.
13. Er worden passende technische (beveiligings-) maatregelen genomen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.
14. Alle beveiligingsincidenten en datalekken worden vastgelegd, volgens een vast protocol afgehandeld en gemeld bij de Autoriteit Persoonsgegevens en zo nodig de personen waarvan de persoonsgegevens hierdoor onbeveiligd waren.

4.2. Relevante wet- en regelgeving

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

- Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur VO
- Wet op het onderwijstoezicht
- Leerplichtwet
- Wet register onderwijsdeelnemers
- Algemene Verordening Gegevensbescherming
- Archiefwet
- Wet medezeggenschap op scholen
- Auteurswet
- Wetboek van Strafrecht
- CAO VO
- Wet College voor toetsen en examens
- Convenant Digitale Onderwijsmiddelen en Privacy

Verder werken wij conform de internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002. Deze norm beschrijft hoe procesmatig kan worden omgegaan met het beveiligen van informatie, met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie binnen de organisatie zeker te stellen.

4.3. Basisregels voor 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 volgende **vijf vuistregels:**

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: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene of gerechtvaardigd belang.

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

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

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

5. Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande uitgangspunten.

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. Onderdeel van het beleid is de regelmatig terugkerende informatie richting medewerkers, leerlingen, ouders en andere betrokkenen. Op de website van de bij de Pontis Onderwijsgroep aangesloten scholen zijn de actuele beleidsdocumenten opgenomen en bestuur en directies van de scholen zorgen er voor dat dit onderwerp regelmatig voor het voetlicht komt bij degenen die te maken hebben met het verwerken van persoonsgegevens.

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 in- formatiebeveiliging 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 (beveiligings)incidenten kunnen worden gemeld bij de privacymeldpunten van de scholen, te weten privacy@pontis.nl. 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 loopt via een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister.

5.5. Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het College van Bestuur en jaarlijks getoetst door de accountant. 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 de Pontis Onderwijsgroep 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.

5.6. Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG is aangesteld door het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.
In het geval medewerkers nalaten te doen waar zij verantwoordelijk voor zijn (plichtsverzuim) kan door bestuur en/of schooldirecties een sanctie worden opgelegd.

De Pontis Onderwijsgroep wordt beoordeeld op de naleving van de AVG door de FG. De laatste beoordeling (april 2020) gaf bij beide scholen van de Pontis Onderwijsgroep een volwassenheidsniveau van 3 (op een schaal van 5) te zien. Dit betekent dat het beleid bij alle betrokken medewerkers, leerlingen en externen bekend is. Maatstaf voor de FG is 4: 'IBP is onderdeel geworden van de PDCA cyclus'.

Om ambitie 4 te halen moeten er nog stappen worden gezet. De belangrijkste zaken om op te pakken zijn:

- Aandacht om de AVG bewustwording onder medewerkers permanent te vergoten.
- De risico's rondom IBP en beheersing hiervan zowel op organisatieniveau als op procesniveau (vooronderzoek verwerkers, aan welke derde partijen worden gegevens verstrekt, inrichting PDCA).
- Organisatie van het aantoonbaar in control zijn en blijven op naleving van de AVG en IBP risico's.

Deze punten zijn opgenomen in de jaarplanning.

In het voorjaar van 2023 volgt een nieuwe monitoring die zal worden vastgelegd in een FG-monitoringsrapportage.

6. Organisatie - Wie doet wat?

6.1. Rollen en verantwoordelijkheden

In dit hoofdstuk wordt beschreven hoe het IBP-beleid binnen de Pontis Onderwijsgroep is georganiseerd. Er vindt daarbij een verdeling van rollen, verantwoordelijkheden en taken plaats op drie niveaus:

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

6.2. Richtinggevende rol (strategisch)

De voorzitter van het College van Bestuur is eindverantwoordelijk voor het IBP-beleid en stelt – in overleg met de schooldirecties en na instemming van de GMR – 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)

- **Werkgroep IBP (uitvoerend en adviserend richting CvB)**

De ondersteuning en aansturing van IBP is bij de Pontis Onderwijsgroep belegd bij de werkgroep IBP als onderdeel van de 'gewone' bedrijfsvoering. De werkgroep bestaat uit het hoofd van Team KIC, de Privacy Officer (PO), de Security Officers (SO) en vertegenwoordigers van de schooladministraties. De werkgroep adviseert en ondersteunt en doet voorstellen t.a.v. het IBP-beleid en de (praktische) invulling hiervan.

- **Privacy Officer (PO)**

Taken PO:

- geeft terugkoppeling en advies aan de eindverantwoordelijke (voorzitter CvB);
- vertaalt het beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling en houdt deze up-to-date;
- bewaakt de uniformiteit binnen de Pontis Onderwijsgroep;
- is het aanspreekpunt voor incidenten op het gebied van informatiebeveiliging en privacy;
- initieert IBP-activiteiten en stelt de jaarplanning op;
- handelt bij incidenten op het gebied van IBP (samen met hoofd KIC en Security Officers).
- is vraagbaak op het gebied van IBP (privacy@pontis.nl)

De rol van PO wordt binnen de Pontis Onderwijsgroep College ingevuld door de bestuursassistent. De PO neemt deel aan de netwerkgroep IBP van de TOP- groep.

- **Security Officer (SO)**

De SO geeft terugkoppeling en advies aan de eindverantwoordelijke (voorzitter CvB). De SO vormt het technisch aanspreekpunt inzake informatiebeveiliging voor schoolleiding en de medewerkers. De SO werkt nauw samen met Privacy Officer en de (leerling)administratie.

- **Functionaris voor Gegevensbescherming**

De functionaris voor gegevensbescherming (FG) houdt binnen de Pontis Onderwijsgroep 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 CvB). De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.
Onze Functionaris Gegevensbeheer LP2 is bereikbaar via fg@L2P.nl.

- **Proceseigenaren**

Binnen de school zijn er verschillende processen, zoals (leerlingen)administratie, ICT, personeel, facilitaire en financiële zaken. Voor 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. Uitvoerende rol (operationeel)

- **Leidinggevenden (o.a. teamleiders, hoofden administraties, hoofden binnen de Centrale Ondersteunende Diensten)**

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

- **Medewerkers OP en OOP**

Elke medewerker heeft verantwoordelijkheden met betrekking tot informatiebeveiliging in zijn of haar dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in onder meer de gedragscode en het protocol ICT (Regius College).
Medewerkers worden gestimuleerd om actief betrokken te zijn bij informatiebeveiliging en actief kennis te nemen van de beschikbare documentatie. Het is daarbij belangrijk dat medewerkers direct melding maken van datalekken en veiligheidsincidenten en zo mogelijk komen met voorstellen tot verbetering van (onderdelen van) procedures voor gegevensverwerking.

Bijlage 1 – overzicht rollen, taken en verantwoordelijkheden

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	CvB	• Eindverantwoordelijk voor IBP • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Aanstellen FG-er	• Informatiebeveiligings- en privacybeleid vaststellen • Inrichten IBP organisatie • Basismaatregelen nemen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend / uitvoerend	**Werkgroep Privacy** Bestaande uit: Privacy Officer Security Officer Vertegenwoordigers schooladministraties	• IBP-planning en controle • Adviseert CvB over IBP • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Deelname netwerk IBP van Topgroep	• Opstellen jaarplanning. • Actualiseren van processen, richtlijnen en procedures . • Verwerkingsregister opstellen en actueel houden. • Afwikkelen klachten en incidenten
	Privacy Officer		• Incidentafhandeling (registreren en evalueren). • vertaalt het beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling. • Neemt deel aan regionaal netwerk IBP • Aanspreekpunt binnen organisatie • Agenderen stukken etc. in COD en GMR
	Security Officer		• Technisch aanspreekpunt voor IBP. Incidentafhandeling op technisch gebied (met afdeling ICT)
	Team Informatiemanagement **waar nodig in samenwerking met proceseigenaren**	• Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door CvB • Er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • De toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); bewerkersovereenkomsten opstellen en registeren. • Risico-analyse • Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: ○ Toegangsmatrix

		• Naleving IBP in de primaire processen • Beheer en inrichting cameratoezicht • Etc.	
	Functionaris voor Gegevensbescherming	• Toezicht op naleving privacy wetgeving • Aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten • Zie de functieomschrijving zoals opgesteld door de VO raad	• Is aangesteld door CvB in samenwerking met meerdere Topgroep scholen.
	Medewerker	• Verantwoordelijk omgaan met IBP bij de dagelijkse werkzaamheden. • Pro-actieve houding om informatie, documentatie, regelingen etc. t.a.v. IPB tot zich te nemen.	Naleving IBP bij werkzaamheden voor het Regius College (op school en thuis).
	Leidinggevend Directie/schoolleiders/ hoofden afdelingen	• Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken

Bijlage 2 – Jaarplanning IBP-activiteiten 2022-2023

Periode	Actie	Uitvoering	Status	
Juni 2022	Opstelling jaarplanning IBP 2022-2023			*Gereed*
Continue	Controle AVG-checklist en actie naar aanleiding hiervan	Werkgroep		
Continue	Deelname AVG netwerk topgroep scholen	PRA		*Loopt*
Continue	Periodiek overleg IBP werkgroep Pontis	Werkgroep		*Loopt*
Juni 2022	Afstemming systeem toestemming: Somtoday?? Leerlingenadministratie vragen om na te bellen. Wendy heeft afspraak met Ruud. Esther checkt bij lladm. TC	Werkgroep	Ouders zijn alleen opgenomen in het WIS portaal De formuliermogelijkheid is er niet in SOMToday Elo. We houden WIS dit jaar – de bredere vraag ligt bij informatiemanagement	*Gereed*
0-week augustus	Informeren nieuwe docenten over AVG Presentatie tijdens kennismaking door Jan op Regius, Michiel HF en Esther JB (26 augustus)			*Gereed*
Nov. 2022	Aanpassen documenten Pontis breed – Beleidsplan Pontis breed – Na instemming GMR interne communicatie via Nieuwsbrief/dagbericht. Externe communicatie via Nieuwsbrief ouders/website.	PRA	Concept gereed	*Concept gereed tbv GMR maart 2023*
Dec. 2022	Aanpassen documenten Pontis breed – Privacyreglement – Privacyverklaring – Na instemming GMR interne communicatie via Nieuwsbrief/dagbericht. Externe communicatie via Nieuwsbrief ouders/website.	PRA		*Concept gereed GMR maart 2023*
2022-2023	DPIA Teams landelijk – Interne maatregelen/risicoafweging	SO	In AVG overleg november stand van zaken afstemmen	*In bewerking team IM*
Nov. 2022 Start 2023	Bewustwording: vervolg AVG online trainingsmodules – Nieuwe collega's – Vervolg/verdieping – Communicatie	Werkgroep	Afspraak november om voortgang te bespreken. Eerste afstemming AVG-trainingen heeft plaatsgevonden. Voorjaar 2023 verdieping uitzetten	*Loopt*

2022-2023	Afstemming inrichting/registratie verwerkersovereenkomsten	PRA / WRF	Pontis verwerkersovereenkomsten Beoordeling leermiddelen via ICT/applicatiebeheer: communicatie via nieuwsbrief	*Loopt*
Begin 2023 doorlopend	Beoordeling diverse documenten (zie ook overzicht hieronder) – Pontis breed opstellen of afzonderlijk? Vervolgens in jaarplanning opnemen: nieuw op te stellen Pontis / actualisatie per school? – Wie doet wat	Werkgroep	*Cameratoezicht* *Privacyreglementen personeel / leerlingen-ouders* *Privacyverklaringen* *Procedure rechten: inrichting procedure* *Procedure bewaartermijnen* *Protocol datalek: inrichting procedure* *Incidentenregister* *Verwerkingsregister*	*Loopt*
Dec. 2022	Privacyverklaring sollicitanten: afstemming P&O en plaatsen op vacaturesite	PRA		*Concept gereed*
Nog te plannen	Verdere implementatie bewaartermijnen: – Somtoday: termijnen afstemmen – Afas: afspraak maken inregelen – interne communicatie	Werkgroep		
Oktober 2022-rest schooljaar	Structurele aandacht voor bewustwording medewerkers – Vervolg AVG training online – Periodieke nieuwsbrieven opstellen/opnemen nieuws in Nieuwsbrief Pontis – Openstellen nieuw Pontisbreed mailadres privacy@pontis.nl	Werkgroep		*Loopt* *Gereed*
Maart 2023	AVG monitoring door FG-er Lumen: voorbereiden documenten	PRA/werkgroep		*Maart/mei 2023* *Loopt*
Jan. 2023	Opstellen jaarverslag voorjaar 2022	PRA		*Gereed*
Mei 2023	AVG nieuws Regius voor nieuwe leerlingen/ouders waar nodig herzien	PRA	*Juni 2022 meegeven aan nieuwe leerlingen/ouders*	
Juni 2023	Opstellen jaarplanning 2022-2023 aan de hand van AVG-checkplan			*Juni 2023*

Bijlage 3 – Overzicht ondersteunende documenten en protocollen

Nr.	Document/regeling	Regius College	Trinitas College	Pontis Onderwijsgroep Deze kolom wordt nog verder ingevuld aan de hand van de jaarplanning
1.	IBP-beleid	Pontisbreed	Pontisbreed	Vastgesteld 12 april 2023
2.	Jaarplanning	*Pontisbreed*	Pontisbreed	Gereed
3.	Privacyreglement	Pontisbreed	Pontisbreed	Vastgesteld 12 april 2023
4.	Privacyverklaring leerlingen en ouders	14 mei 2018 *Versie 2: Actualisatie: oktober 2020*	Versie 08-01-2020	Concept gereed t.b.v. GMR
5.	Privacyverklaring medewerkers	*Pontisbreed*	*Pontisbreed*	Concept gereed
6.	Privacyverklaring sollicitanten	*Pontisbreed*	*Pontisbreed*	Concept gereed
7.	Interne procedure rechten betrokkenen	30 mei 2018	Juni 2018 Een werkwijze is afgestemd tussen PO en administraties/P&O	Schooljaar 22-23 samenvoegen
8.	Autorisatiematrix SomToday en AFAS	Som Today ja/in ontwikkeling	Nee	
9.	Register verwerkingsactiviteiten leerlingen/ouders	Mei 2019 *Wordt steeds aangevuld bij nieuwe verwerkersovereenkomsten* *Actualisatie: november 2020*	Versie 2. 26-02-2020 Geactualiseerd bij nieuwe overeenkomst	Concept Pontis in bewerking
10.	Verwerkersovereenkomsten en - registratie	Continue	Continue	Nieuwe Pontis registratie opgezet. Nieuwe verwerkersovereenkomsten conform versie 4.0.
11.	Handboek datalekken	December 2020	April 2018	Schooljaar 23-24

12.	ICT protocol Richtlijnen voor gebruik internet en audio	April 2021	April 2018	Samenvoegen? Nagaan schooljaar 23-24
13.	Protocol bewaartermijnen	Maart 2021	Concept	Schooljaar 23-24
14.	Protocol cameratoezicht	November 2020	Oktober 2019	Schooljaar 23-24