Informatiebeveiligings- en Privacybeleid Regius College Schagen

Versie	Datum		Naam	Functie
1	mei 2018		A.H. Hoekstra	voorzitter CvB
1.1	november 2019	update		
1.2	oktober 2020	actualisatie	A.H. Hoekstra	voorzitter CvB

Instemming versie 1.1 GMR d.d.: 29 mei 2018
Instemming versie 1.2 GMR d.d. 17 november 2020

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.
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. 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 Regius College Schagen (hierna te noemen: Regius College) 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:

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

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn 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 Regius College voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen het Regius College geldt voor alle medewerkers, tijdelijk personeel, 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 betrokkenen binnen het Regius College waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan het Regius College persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het Regius College.
- Het IBP-beleid geldt voor de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van

het Regius College 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.

- Het IBP-beleid heeft binnen het Regius College 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, digitale leermiddelen
    - Toets- en examenbeleid, voorkomen van fraude
    - Doorstroomgegevens uitwisselen met basisscholen en vervolgonderwijs.

4. Beleid – uitgangspunten

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

1. Het schoolbestuur van het Regius College 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. Het Regius College voldoet aan alle relevante wet- en regelgeving.

3. Bij het Regius College 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 Regius College 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.

4. Het Regius College 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, data-portabiliteit en profilering.

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

6. Binnen het Regius College 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. Het Regius College 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 en de benodigde investeringen en de te nemen maatregelen.

9. Het Regius maakt met partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over de informatiebeveiliging en privacy (middels een verwerkersovereenkomst).

10. Informatiebeveiliging en privacy is bij het Regius College een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

11. Het Regius College 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.

12. Het Regius College 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.

13. Het Regius College zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en 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:

- Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht
- CAO VO
- Wet Passend Onderwijs
- Examens en toetsing (gepubliceerd op Examenblad.nl)

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is 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.

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:

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 (subsidiar). 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 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. Binnen het Regius Dashboard is een privacybutton opgenomen waaronder alle actuele documenten staan geplaatst. Daarnaast zullen er (online) trainingen worden verzorgd voor de medewerkers en wordt periodiek een nieuwsbrief 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 beveiligingsmaat-

regelen 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 (beveiligings)incidenten kunnen worden gemeld bij privacy@regiuscollege.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 volgt 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 voor 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 het Regius College 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

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 Regius College wordt beoordeeld op de naleving van de AVG door de FG. De laatste beoordeling vond plaats in april 2020. Hieruit blijkt dat het RegiusCollege een volwassenheidsniveau 3 op een schaal van 5 scoort. 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 processniveau (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 zaken zijn opgenomen in de jaarplanning 2020-2021. Ook doet het Regius College eind 2020 mee met de AVG steekproef van Lumen Group. Lumen Group maakt hiervan een rapportage en bespreekt de bevindingen en aanbevelingen

6. Organisatie – Wie doet wat?

6.1 Rollen en verantwoordelijkheden

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij het Regius College 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 Regius College wordt georganiseerd.

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

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

Richtinggevende rol (strategisch)

Het College van Bestuur is eindverantwoordelijk voor het IBP-beleid en stelt – in overleg met de sectordirecties – 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.

Sturende rol (tactisch) / Uitvoerende rol (operationeel)

Werkgroep IBP (uitvoerend en adviserend richting CvB)

De ondersteuning en aansturing van IBP is bij het Regius College belegd bij de werkgroep IBP als onderdeel van de 'gewone' bedrijfsvoering. De werkgroep bestaat uit de **Privacy Officer (PO)** ,de **Security Officer (SO) en het hoofd administratie**.
De werkgroep adviseert en ondersteunt en doet voorstellen t.a.v. het IBP-beleid en de (praktische) invulling hiervan.

Privacy Officer (PO)

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

- geeft terugkoppeling en advies aan de eindverantwoordelijke (het CvB);
- vertaalt het beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling en houdt deze up-to-date;
- bewaakt de uniformiteit binnen het Regius College;
- 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 (met hoofd ICT, security officer).
- is vraagbaak op het gebied van IBP (privacy@regiuscollege.nl)

De rol van PO wordt binnen het Regius College ingevuld door de bestuursondersteuner.
De PO en het hoofd sectoradministratie nemen deel aan de netwerkgroep IBP van de TOP-groep.

Security Officer (SO)

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

Hoofd ICT

De werkzaamheden van de afdeling ICT bestrijken een breed gebied van ICT in onderwijs en bedrijfsvoering; informatiebeveiliging en privacy is één van de aandachtspunten. Het hoofd ICT adviseert samen met de Security Officer het College van Bestuur en ziet toe – mede namens de sectordirecteuren – op de naleving van het IBP-beleid in de primaire processen van het Regius College.

De afdeling ICT speelt een rol in het opstellen van de autorisatiematrix/het toegangsbeleid, verwerkingsregisters, risicoanalyse etc.

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen het Regius College 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 informatiebe-

veiligingsincidenten, 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.

Wij hebben een externe Functionaris voor de Gegevensbescherming (FG) aangesteld, te weten Peter Tanamal van Lumen Group.

Contactgegevens: FG@lumengroup.nl of via de link naar het contactformulier: https://www.lumengroup.nl/contact-fg/

Proceseigenaren

Binnen de school zijn er verschillende processen, zoals (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.

Uitvoerende rol (operationeel)

Leidinggevenden (sectordirecteuren, teamleiders, hoofd sectoradministratie, hoofd financiën etc.)

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 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 de button Privacy op het Regius Dashboard). Medewerkers maken melding van datalekken en veiligheidsincidenten, doen verbetervoorstellen etc.

Overzicht rollen, verantwoordelijkheden en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	CvB	• Eindverantwoordelijk • 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 Hoofd sectoradministratie Hoofd ICT sluit periodiek aan.	• 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 schoolleiding en GMR

	Security Officer		• Technisch aanspreekpunt voor IBP. Incidentafhandeling op technisch gebied (met afdeling ICT)
	Afdeling/hoofd ICT **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. • Naleving IBP in de primaire processen • • Beheer en inrichting camera-toezicht • Etc.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); bewerkersovereenkomsten opstellen en registeren. • Risico-analyse • Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: ○ Toegangsmatrix
	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).

	Schoollei-ding/teamleiders/ hoofden afdelingen	• Communicatie naar alle be-trokkenen; 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, richt-lijnen en procedures door de medewerkers. • Voorbeeldfunctie met posi-tieve en actieve houding t.a.v. IBP-beleid. periodiek het onderwerp in-formatiebeveiliging onder de aandacht te brengen in werk-overleggen, beoordelingen etc.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dos-siers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken

Bijlage 1: Ondersteunende documenten en procedures

Nr.	Document/regeling	Datum vaststelling	Website	Regius Dashboard
1.	IBP-beleid	Mei 2018 *Versie 2: Actualisatie: september 2019* *Versie 3: Actualisatie: november 2020*	Ja	Ja
2.	Jaarplanning	September 2020	Nee	Ja
3.	Privacyreglement	14 mei 2018 *Versie 2: Actualisatie: oktober 2020*	Ja	Ja
4.	Privacyverklaring leerlingen en ouders	14 mei 2018 *Versie 2: Actualisatie: oktober 2020*	Ja	Nee
5.	Privacyverklaring medewerkers	November 2020	Nee	Ja
6.	Privacyverklaring sollicitanten	November 2020	Ja	Nee
7.	Interne procedure inzagerecht ouders/leerlingen	30 mei 2018	Nee	Ja
8.	Autorisatiematrix SomToday en AFAS	In ontwikkeling	Nee	Nee
9.	Register verwerkingsactiviteiten leerlingen/ouders	Mei 2019 *Wordt steeds aangevuld bij nieuwe verwerkersovereenkomsten* *Actualisatie: november 2020*	Nee	Ja
10.	Verwerkersovereenkomsten en - registratie	Continue	Nee	Ja
11.	Register verwerkingsactiviteiten personeel	November 2019 *Wordt steeds aangevuld bij nieuwe verwerkersovereenkomsten* *Actualisatie: november 2020*	Nee	Ja
12.	FG reglement	29 januari 2020	Nee	Nee
13.	Protocol gebruik van camera- en videobeelden	4 juni 2018 *Actualisatie: november 2020*	Ja	Ja
14.	Geheimhoudingsverklaring (o.a. gedetacheerden, Parlan, SWV, uitzendkrachten, surveillanten, vrijwilligers, stagiaires, studenten etc.)	November 2020	Nee	Nee
15.	Toestemmingsprocedure leerlingen	Procedure juni 2019 Uitvraag en archivering via AVG module van Wis	Nee	Ja
16.	Protocol datalekken	4 juni 2018 *Actualisatie: december 2020*	Nee	Ja
17.	Protocol bewaartermijnen	December 2020		Ja
18.	Disclaimer bezoekers website	Juni 2018		
19.	Protocol ICT	December 2020	Nee	Ja