Informatiebeveiligings- en Privacybeleid Regius College Schagen

Vastgesteld CvB d.d.: 17 mei 2018
Instemming GMR d.d.: 29 mei 2018

Inhoudsopgave

Bron: Kennisnet

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, 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. 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 (bijvoorbeeld 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 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 en (digitale) leermiddelen.
  - *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers.

4. Beleid – Hoe doen we dat?

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, inza-

ge, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit 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 geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. Het Regius College classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

9. Het Regius College sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) 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.

10. Het Regius College 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. Het Regius College heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

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

12. 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.

13. 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.

14. 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.

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 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.

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 de **vijf vuistregels** met be-

trekking 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.

5.3 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. Een aantal protocollen en procedures die relevant zijn voor het IBP-beleid bestaan al, maar moeten nog worden getoetst aan het nieuwe IBP-beleid en zo nodig aangepast.
De planning voor alle te ontwikkelen of bij te stellen protocollen, documenten etc., die in dit document worden genoemd, zijn in bijlage 2 opgenomen in de actiepuntenlijst.

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

5.4 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 zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers en leerlingen.

5.5 Classificatie en 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.

5.6 Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in 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 bij privacy@regiuscollege.nl.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7 Planning en controle

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

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

Daarnaast kent het Regius College een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud

en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

5.8 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. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
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. De FG werkt via een door het bestuur vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan het Regius College de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de reglementen van het Regius College, de CAO en de wettelijke mogelijkheden.

5.9 Logging en monitoring

Logging en monitoring door de afdeling systeembeheer zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

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)

Projectgroep IBP (uitvoerend en adviserend richting CvB en ICT-werkgroep)

De ondersteuning en aansturing van IBP is bij het Regius College belegd bij de Projectgroep IBP. De projectgroep bestaat uit een **Privacy Officer/PO** en een **Security Officer/SO** en staat onder aansturing van de voorzitter van het CvB.

De projectgroep adviseert en ondersteunt en doet voorstellen t.a.v. het IBP-beleid, Privacyreglement, verwerkingsactiviteiten en andere IBP-documenten. Dit project loopt totdat de implementatiefase is doorlopen en de activiteiten, zoals benoemd in bijlage 1, zijn afgerond; IBP is dan onderdeel van de 'gewone' bedrijfsvoering.

Privacy Officer (PO)

De PO geeft terugkoppeling en advies aan de eindverantwoordelijke (het CvB). De PO:

- vertaalt het beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling;
- bewaakt de uniformiteit binnen het Regius College;
- is het aanspreekpunt voor incidenten op het gebied van informatiebeveiliging en privacy;
- coördineert de verdere afhandeling van incidenten binnen het Regius College.

Security Officer (SO)

De SO geeft terugkoppeling en advies aan de eindverantwoordelijke (het CvB). De Security Officer (SO) vormt het technisch aanspreekpunt inzake informatiebeveiliging voor schoolleiding en de medewerkers. De SO rapporteert aan de voorzitter van het CvB.

ICT werkgroep

De ICT werkgroep bestaat uit de voorzitter van het CvB, portefeuillehouders vanuit de sectordirecties, teamleiders, systeembeheer, applicatiebeheer en een docent. De agenda van de werkgroep ICT bestrijkt een breed terrein van ICT in onderwijs en bedrijfsvoering; informatiebeveiliging en privacy is één van de aandachtspunten. De werkgroep adviseert samen met de Security Officer het College van Bestuur en is – mede namens de collega-sectordirecteuren – verantwoordelijk voor de naleving van het IBP-beleid in de primaire processen van het Regius College.

De projectgroep IBP en de ICT werkgroep werken samen met name bij zaken als het opstellen van een autorisatiematrix, verwerkingsregisters, BIV classificaties, 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 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.

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.

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

- samen met de werkgroep ICT stellen zij het beleid voor toegang tot de informatiesystemen vast.
- samen met de werkgroep ICT zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- samen met de werkgroep ICT beoordelen zij regelmatig de toegangsrechten van gebruikers.

Uitvoerende rol (operationeel)

Leidinggevenden (CvB, 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.
Medewerkers worden gestimuleerd om actief betrokken te zijn bij informatiebeveiliging en actief kennis te nemen van de beschikbare documentatie. Medewerkers maken melding van veiligheidsincidenten, doen verbetervoorstellen etc.

Overzicht rollen, verantwoordelijkheden en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Voorbeelden: 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 • Organisatie IBP inrichten • Aanstellen FG-er	• Informatiebeveiligings- en privacybeleid vaststellen • Inrichten IBP organisatie • Basismaatregelen nemen • Reglement FG vaststellen • Privacyreglement vaststellen

Sturend / uitvoerend	**Projectgroep Privacy**	• IBP-planning en controle • Adviseert CvB over IBP • Voorbereiden uitvoering IBP-beleid, Classificatie (SO) en risicoanalyse (SO/PO/CvB) • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Opstellen concepten voor: • IBP-beleidsplan • activiteitenkalender (zie bijlage 1) • processen, richtlijnen en procedures IBP (zie bijlage 2)
	ICT-werkgroep **waar nodig in samenwerking met proceseigenaren waaronder o.a.:** **ICT,** **P&O,** **facilitair,** **onderwijs,** **financiën,** **sectoradministratie en leerlingenadministratie.**	• 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. • Verwerkingsregister opstellen en actueel houden. • Classificatie- en risicoanalyse documenten, opgesteld door CvB en projectteam IBP beoordelen en aanpassen. • Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: o Toegangsmatrix
	Functionaris voor Gegevensbescherming	• Toezicht op naleving privacy wetgeving • Aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Wordt aangesteld door CvB in samenwerking met meerdere Topgroep scholen.

	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	
	Security Officer	• Technisch aanspreekpunt voor IBP.	
	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 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. • Samen met projectgroep/ICT werkgroep implementeren IBP-maatregelen. 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 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht. Dit overzicht wordt regelmatig geactualiseerd aangezien diverse regelingen nog in ontwikkeling zijn (zie bijlage 2 – actieplan).

Document/regeling	Gereed d.d.	SL	GMR + status
▪ Privacyreglement Regius College Schagen	14 mei 2018	17 mei 2018	29 mei goedgekeurd
▪ Procedure inzagerecht ouders/leerlingen	30 mei 2018	–	–
▪ Risico-analyse			
▪ Autorisatiematrix SomToday en AFAS			
▪ Register verwerkingsactiviteiten (inclusief BIV classificatie) en bewaartermijnen			
▪ Gegevensbeschermingseffectbeoordeling (GEB)			
▪ Protocol gebruik e-mail, internet en sociale media / EICM			
▪ Protocol gebruik van camera- en videobeelden	4 juni 2018	14 juni 2018	26 juni 2018
▪ Geheimhoudingsverklaring			
▪ Informatie- en toestemmingsformulier voorafgaand aan gegevensverwerking (waaronder gebruik beeldmateriaal etc.)			
▪ Modelantwoord op een verzoek ex artikel 15AVG (leerlingen/personeel)			
▪ Verwerkersovereenkomsten en - registratie			
▪ Protocol datalekken	4 juni 2018	14 juni 2018	26 juni 2018
▪ Privacyverklaring	28 mei 2018	14 juni 2018	26 juni 2018

Bijlage 2: Actieplan

NR	Actie	Omschrijving	Status	wie	wanneer gereed
1.	**IBP-beleid en aanpak**				
1.1	Informatie- en Privacybeleid opstellen	▪ Opstellen Beleidsplan IBP. Bijlage is deze actielijst ▪ De IBP-organisatie is ingericht (taken en rollen) waarbij verantwoordelijkheden en taken zijn belegd bij medewerkers.	▪ Concept gereed 5 mei ▪ Concept in SL 17 mei ▪ Inbrengen in GMR 29 mei ter **instemming**	Voorzitter CvB / PO	April 2018 Mei 2018 Mei/juni 2018
1.2	Aanstellen Functionaris gegevensbescherming	Dit mag ook iemand zijn buiten de organisatie.	In onderzoekende fase/in samenspraak met TOPgroep	Topgroep CvB	September 2018
1.3	Projectgroep samenstellen	De functiebenamingen zoals gebruikt in IBP aanpak worden gevolgd.	**Eindverantwoordelijk:** voorzitter CvB **Projectgroep IBP** (uitvoerend en adviserend richting CvB en ICT-werkgroep) bestaat uit Privacy Officer/PO (Wendy Pranger) en Security Officer/SO (Henrie van der Meer) onder aansturing van de voorzitter van het CvB. **ICT werkgroep** bestaat uit voorzitter CvB, portefeuillehouders vanuit de sectordirecties, teamleiders, systeembeheer, applicatiebeheer en een docent.	Voorzitter CvB	gereed

1.4	IBP opnemen in planning- en controlcyclus			SL	
2.	**Opstellen documenten (na instemming altijd nagaan hoe documenten intern/extern gecommuniceerd worden)**				
2.1	Beleidsplan IBP		▪ Concept gereed 5 mei ▪ Concept in SL 17 mei ▪ Inbrengen in GMR 29 mei ter **instemming** ▪ Communicatie in- en extern	Voorzitter CvB / PO	April 2018 Mei 2018 Mei/juni 2018
2.2	Privacyreglement	Privacyreglement opstellen	▪ Concept gereed 5 mei ▪ Concept in SL 17 mei ▪ Inbrengen in GMR 29 mei ter **instemming** ▪ Communicatie in- en extern	Voorzitter CvB / PO	April 2018 Mei 2018 Mei/juni 2018
2.3	Procedure Datalekken	Procedure datalekken opstellen met onder-meer: ▪ protocol beveiligingsincidenten/datalekken (werkwijze) ▪ meldformulier Inrichten: ▪ meldpunt voor beveiligingsincidenten en datalekken ▪ registratie datalekken	▪ Concept gereed 25 mei ▪ Concept in SL 14 juni ▪ Inbrengen in GMR vergadering juni 2018 of eerste vergadering schooljaar 2018-2019 ter **instemming** ▪ Communicatie in- en extern	Voorzitter CvB / PO	Juni 2018 Najaar 2018
2.	Geheimhoudingsovereen-	voor medewerkers die niet onder CAO vallen (zoals gedetacheerden, Parlan, SWV, uit-	▪ Concept gereed september 2018	Voorzitter CvB / PO	September 2018

4	komst	zendkrachten, surveillanten, vrijwilligers)			
2.5	Toestemming gebruik foto's/video's etc. Informatie-/ toestemmingsformulier	▪ Dit formulier wordt uitgezet 'voor onbepaalde tijd' met mogelijkheid tot opzegging. ▪ Ieder jaar herhaling van bericht. ▪ Toestemming aantoonbaar registeren.	▪ Toestemmingsformulier in juni gereed ▪ Afstemming systeembeheer (Google formulier via Ouderweb) ▪ Inbrengen in SL ▪ In eerste instantie maken we foto's van een groep van ca. 30 leerlingen die gedurende het jaar te gebruiken zijn.	Voorzitter CvB / PO	Juni 2018
2.6	Protocol gebruik van camera- en videobeelden.	Protocol waarin wordt aangegeven hoe we hiermee omgaan, welke termijnen we hanteren en wie welke rechten heeft	▪ Concept gereed juni 2018 ▪ Inbrengen in SL ▪ Afstemming met betrokkenen (conciërges etc.)	Voorzitter CvB / PO	September 2018
2.7	Privacyverklaring	Opstellen van een beknopte en toegankelijke privacyverklaring en direct beschikbaar maken voor betrokkene(n) (op website en/of schoolgids).	▪ Concept gereed begin 22 mei ▪ Concept in SL 14 juni	PO	Juni 2018
2.8	Opt out procedure	Recht om vergeten te worden. Voor leerlingen/ouders die schoolverlaten,	▪ Procedure staat beschreven in privacyreglement. ▪ Intern afstemmen/inrichten.	PO	September 2018
2.9	Inzagerecht (procedure) voor ouders/leerlingen en personeel		▪ Procedure staat beschreven in privacyreglement. ▪ Intern afstemmen/inrichten. ▪ Antwoordbrief opstellen	PO	September 2018

3.	**Waar nodig aanpassen bestaande documenten aan IBP-beleid**				
3.1	Protocol EICM	Doorlopen op avg-regels (zie Modelreglement internet en sociale media voor leerlingen en medewerkers op Kennisnet en Wille Donkers) Aandacht voor leerlingen < 16 jaar ivm toestemming bij gebruik sociale media	▪ Najaar 2018 ▪ Inbrengen in SL ▪ Afhankelijk van aanpassingen ter informatie of ter instemming naar GMR	PO	Najaar 2018
3.2	Gedragscode personeel	Gedragscode personeel nakijken (zie gedragscode ICT/ handreiking verantwoord gebruik van bedrijfsmiddelen voor medewerkers)	▪ Najaar 2018 ▪ Inbrengen in SL ▪ Afhankelijk van aanpassingen ter informatie of ter instemming naar GMR	PO	Najaar 2018
3.3	Leerlingstatuut	Doorlopen op avg-regels	▪ Najaar 2018 ▪ Inbrengen in SL ▪ Afhankelijk van aanpassingen ter informatie of ter instemming naar GMR	PO	Najaar 2018
3.4	Overige documenten nakijken	Bestaande regelingen doorlopen of deze voldoen aan IBP beleid.		PO	Najaar 2018

4.	**Risico analyse / technische en organisatorische maatregelen**				
4.1	Gegevensvastlegging en classificatie (BIV)	Overzicht van alle informatiesystemen die gegevens bevatten met het doel van de vastlegging en de classificatie	▪ BIV classificatie gegevens in verwerkersbestand opnemen. ▪ Mogelijk later classificatie systemen (advies FG) ▪ Inbrengen in ICT werkgroep ▪ GMR ter informatie.	Projectgroep / SO ICT werkgroep	
4.2	Risico-analyse	Beschrijving mogelijke risico's met kans en impact. Op basis van deze risico's worden maatregelen (die reeds zijn ingevoerd) beschreven.	▪ Zie voorbeeld Jan Arentsz ▪ Wendy bereidt basisdocument voor ▪ Voorzitter CvB en projectgroep vullen het bestand in aan de hand van handleiding ▪ Bestand inbrengen in ICT werkgroep ▪ GMR ter informatie	Projectgroep ICT werkgroep	
4.3	Gegevensbeschermings-effectbeoordelingen (GEB)	Onderzoeken bij welke verwerkingsactiviteiten een GEB noodzakelijk is	Alleen bij nieuwe systemen? Steeds vooraf bij nieuwe ontwikkelingen/technieken kijken of GEB gedaan moet worden. Informatie volgt nog op kennisnet	Werkgroep ICT?	Najaar 2018
4.4	Technische en organisatorische maatregelen	Zie handreiking handboek Wille Donkers (wordt aangevuld)		Werkgroep ICT	

5.	**Verwerkingsactiviteiten**				
5.1	Inrichten register van verwerkingsactiviteiten (wettelijke verplichting)	In dit register staan de gegevens die voor elk doel wordt verwerkt. Aan het verwerkingregister worden wettelijke eisen gesteld.	Nog besluit nemen over format (voorbeeld beschikbaar vanuit Kennisnet + voorbeeld Wille Donkers) Afstemmen in netwerk Privacy	Werkgroep ICT	Najaar 2018
5.2	Bewaartermijnen	Opstellen document met bewaartermijnen die RC hanteert. Nagaan of we deze termijnen hanteren en zo nodig aanpassingen doen	Overzicht beschikbaar via Wille Donkers	PO	Najaar 2018
5.3	Overzicht van toegangsrechten interne verwerkers	Opstellen overzicht van diegenen die toegang hebben tot de persoonsregistratie van RC zoals bedoeld in artikel 4 van het Privacyreglement	= autorisatiematrix Wordt opgesteld voor SOM AFAS volgt.	SOMToday werkgroep	
5.4	Afspraken met leveranciers	▪ Nagaan met welke leveranciers verwerkersovereenkomsten moeten worden opgesteld. ▪ Privacy bijsluiters van de verwerkersovereenkomsten publiceren (transparantie) ▪ Centraal archiveren overeenkomsten	Gebruik model 3.0 Kennisnet Check of bij de huidige overeenkomsten aan alle voorwaarden is voldaan en evt. actie. tzt aanpassen aan nieuwe opzet. Mag van AP na mei 2018 (centrale afspraken zijn er dan met leveranciers)	Afdeling facilitair in samenwerking met PO	Najaar

6.	**Communicatie / bewustwording**				
6.1	Button Dashboard personeel	▪ Inrichten pagina met informatie, documenten, reactiemogelijkheid, speciaal formulier melden incidenten/datalek ▪ Up to date houden	▪ Systeembeheer vragen button in richten ▪ Communiceren via Regius Info/dagbericht ▪ Regelmatig up to date houden	Projectgroep	Juni 2018 PO
6.2	Voorlichting medewerkers	▪ Via Regius Info/dagbericht ▪ Posters kennisnet ophangen ▪ Via button Regius Dashboard ▪ Presentatie tijdens opening nieuwe schooljaar 2017/2018 ▪ In teams Oud medewerkers toestemming?	Regius Info mei eerste opzet maken	Voorzitter CvB/PO Voorzitter CvB	Mei/juni 2018 September 2018
6.3	Informeren leerlingen en ouders	▪ Informatietekst voor ouders als 'voor-aankondiging' in Regius Nieuws (actief informeren, wijzen op Privacyreglement, rechten betrokkenen etc.) ▪ Toezenden documentatie voor leerlingen, ouders / verzorgers: + 1. Informatie- en toestemmingsformulier voor nieuwe en huidige leerlingen en ouders 2. Toestemmingsformulier oud-leerlingen		Voorzitter CvB/PO	Juni 2018 September 2018

		Aandacht in klas voor wachtwoordbeleid, social media en toestemming, mediawise etc.		ICT werk-groep /SL	
7.	**Website**				
7.1	Privacy statement bezoe-kers website	Beschrijving hoe wij met persoonsgegevens van bezoekers omgaan en deze beveiligen.	Format aanwezig	SO	Juni 2018
7.2	Privacy bij sollicitaties op vacaturepagina	Onderzoeken hoe en of we dit gaan vermel-den		SO	