IBP-beleid

Informatiebeveiliging en privacy

Juli 2023

alma college

Inhoudsopgave

1 Het belang van informatiebeveiliging en privacy

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. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan.
De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Daarbij gaat het om het risico van een beveiligings- of datalek waarbij persoonsgegevens van leerlingen, ouders of medewerkers misbruikt kunnen worden.
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 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 van het Alma College. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

2.2 Privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

2.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk. Daarom worden ze samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis voor informatiebeveiliging en privacy binnen het Alma College en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering van het Alma College.
- Het garanderen van de privacy van alle betrokkenen waarvan het Alma 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 Alma College voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen het Alma College geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). 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 Alma College waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan het Alma College persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Het Alma College. Hieronder valt tevens de gecontroleerde informatie, die door het Alma College is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop het Alma College kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van het Alma 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.

- IBP-beleid heeft binnen het Alma 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;
    - ICT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen;
    - Medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers.

4 Uitgangspunten IBP-beleid

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

1. Het bestuur van het Alma College is verantwoordelijk voor een zorgvuldige regeling van informatiebeveiliging en privacy.
2. Het Alma College voldoet aan alle relevante wet- en regelgeving.
3. Bij het Alma College is de verwerking van persoonsgegevens altijd gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van het Alma 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 Alma 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, dataportabiliteit en profilering.
5. Het Alma College legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Het Alma College voldoet hiermee aan de documentatieplicht.
6. Binnen het Alma 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. De besturen van de moederscholen van het Alma College (PiusX, Het Noordik en Het Erasmus) zijn als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert het Alma College informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. Het Alma 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 Alma College sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de Stichting, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
10. Het Alma College heeft een gedragscode geformuleerd, vastgesteld en geïmplementeerd als het gaat om het veilig en betrouwbaar omgaan met informatie. Het Alma College verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich overeenkomstig deze code 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.
11. Informatiebeveiliging en privacy is bij het Alma College een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Het Alma 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 Alma 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 Alma 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 IBP-beleid

Dit hoofdstuk geeft de praktische invulling van bovenstaande beleidspunten.

5.1 Relevante wet- en regelgeving

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

- Wetgeving:
  - Wet op het voortgezet onderwijs
  - Wet op het onderwijstoezicht
  - Algemene Verordening Gegevensbescherming
  - Archiefwet
  - Leerplichtwet
  - Auteurswet
  - Wetboek van Strafrecht
- De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) (leidend voor de te nemen beveiligingsmaatregelen).
- De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' (leidend bij het maken van afspraken met leveranciers, die in opdracht van de ver-werkingsverantwoordelijke 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 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.
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: het Alma College 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. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

5.4 Voorlichting en bewustzijn

Het beleid en de daarbij behorende 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, leerlingen en bezoekers en externe relaties. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP (netwerk privacy coördinatoren), de FG, de eindverantwoordelijke schoolleiders en het bestuur van het Alma College.

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. Van belang hierbij zijn de beschikbaarheid, de integriteit en de vertrouwelijkheid van de informatie.
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

Elke medewerker, die een beveiligingsincident of datalek vermoedt, dient dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze beveiligingsincidenten en datalekken volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle beveiligingsincidenten en datalekken worden vastgelegd in een incidentenregister. Alle beveiligingsincidenten en datalekken kunnen worden gemeld bij de privacy coördinator of bij de FG.
Periodiek zullen de beveiligingsincidenten en datalekken besproken worden en waar nodig aanvullende en passende beleidsmaatregelen genomen worden.

5.7 planning en controle

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

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

Daarnaast kent het Alma College een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP-beleid 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 Gegevensbescherming (FG) een belangrijke rol. De FG is 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 tekortschieten, dan kan het bestuur van een van de moederscholen de betrokken verantwoordelijke medewerker(s) een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.9 Logging en monitoring

Logging en monitoring door de ICT-afdeling zorgt ervoor 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 van het IBP-beleid

6.1 Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen.

Niveau	Wie? **Rollen**	Hoe? **Verantwoordelijkheid/taken**	Wat? **Realiseren/vastleggen**
Richtinggevend (strategisch)	Bestuur	• 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	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	Verantwoordelijke IBP samen met netwerk privacy coördinatoren onder regie van het CvB	Verantwoordelijk voor concrete uitwerking en uitvoering van IBP beleid, waaronder: • IBP-planning en controle • Adviseren bestuur/directie over IBP • Voorbereiden uitvoeren IBP-beleid, classificatie/risicoanalyse • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens	Processen, richtlijnen en procedures IBP, waaronder: • Protocol beveiligingsincidenten & datalekken • Register van verwerkersovereenkomsten • Protocol toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Formuleren bewustwordingsactiviteiten • Protocol gebruik bedrijfsmiddelen, internet en social media • Protocol social media voor leerlingen
	Privacy coördinator	• Zorgt voor implementatie vastgestelde beleid en procedures op de instelling • Aanspreekpunt en zorgen voor afhandeling privacy klachten en incidenten (en/of datalekken)	• Inrichten meldpunt datalekken • Organiseren bewustwordingsactiviteiten • Inrichten en onderhouden van autorisatiematrix

		• Aanspreekpunt (meldpunt) voor privacy vraagstukken en aangelegenheden op de instelling • Zorgt voor privacy bewustzijn op de instelling	
	Functionaris voor Gegevensbescherming	Toezicht op naleving AVG • informatie verzamelen om verwerkingswerkzaamheden te identificeren; • analyseren en controleren in hoeverre verwerkingswerkzaamheden aan de AVG voldoen; en de verantwoordelijke of de verwerker informeren, adviseren of aanbevelingen geven.	• Onmiddellijke raadpleging bij incidenten. • Betrokken bij alle belangrijke beslissingen rond gegevensbescherming. • Monitoring rapportage opstellen en bespreken met bestuur. • Aanwijzingen geven op basis van de bevindingen van het toezicht.
	Domein-verantwoordelijke/ Proceseigenaren Waaronder o.a.: <u>Bestuursbureau</u> • Advies & Support • Formatie & Financiën • Huisvesting & Facilities, • ICT • Communicatie • Secretariaat <u>Instellingen:</u> • Bedrijfsvoering / DOS • Onderwijs	• Classificatie / risicoanalyse in samenwerking met verantwoordelijke IBP / privacy coördinator • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door CvB • Toezien op toegang tot het netwerk en de netwerkdiensten waarvoor de gebruiker specifiek bevoegd is door applicatiebeheer i.s.m. ICT-beheer Regelmatige beoordeling en controle van de toegangsrechten van gebruikers door functioneel beheer i.s.m. ICT-beheer	• Inventariseren waar persoonsgegevens van het Alma College terechtkomen (leveranciers lijst); input dataregister • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Autorisatiematrix diverse informatiesystemen en netwerk
Uitvoerend (operationeel)	ICT-beheerder	• Inrichten technische beveiligingsmaatregelen • Afhandeling en registratie technische beveiligingsincidenten • Neemt deel in netwerk privacy- coördinatoren. • Technisch aanspreekpunt voor IBP-incidenten. • Adviseert over en draagt zorg voor uitvoering beveiligingsbeleid.	
	Applicatie beheerder	Uitvoeren taken conform gegeven richtlijnen en procedures.	
	Medewerker	• Verantwoordelijk omgaan met IBP bij de dagelijkse	

		werkzaamheden.	
	Dagelijkse leiding / leidinggevende / directie van de instelling en locaties	• 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. • Implementeren IBP-maatregelen. • Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan het bestuur.	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

De verdere uitwerking van de rollen en taken staan beschreven in bijlage 2.

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.

Documenten:	Aandachtspunten:
Procedure toestemming gebruik beeldmateriaal	toestemmingsbrief
Procedure voor verwijderen van gegevens	bewaartermijnen
Communicatie rechten betrokkenen	communicatie richting betrokkenen
Procesbeschrijving rechten betrokkenen	proces rondom aanvragen van betrokkenen
Privacyreglement	
Autorisatiematrix	wie mogen gegevens inzien, bewerken enz.
Afspraken gebruik sociale media	bewustzijn creëren
Procedure rondom training medewerkers	
Cameratoezicht	
Wachtwoordbeleid	
Responsible disclosure	
Gedragscode ICT en internetgebruik	
Acceptable use policy	verantwoord gebruik bedrijfsmiddelen
Procedure rondom uitwisselen gegevens	passend onderwijs, leerling dossiers, leerplicht etc.
Carmel Informatiebeveiligingsbeleid	

Verplicht vanuit de AVG:

Documenten:	Aandachtspunten:
Procesbeschrijving melden datalekken	
Registratie beveiligingsincidenten	
Dataregister om te voldoen aan de registratieplicht	
Verwerkersovereenkomsten	privacy bijlage beschikbaar stellen
Procedure gegevensbeschermings-effectbeoordeling	DPIA
Risicoanalyse	
Functionaris voor Gegevensbescherming	communicatie hierover richting medewerkers

Bijlage 2: Organisatie; wie doet wat

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Stichting Carmelcollege een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen. Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Eindverantwoordelijkheid
Het bestuur is eindverantwoordelijk voor IBP en stelt 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. De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de verantwoordelijke IBP.

Verantwoordelijkheid IBP
Conform artikel 14 van het Bestuursbesluit AVG heeft het managementteam van het Alma College de opdracht de realisatie van alle bepalingen uit het besluit op zich te nemen. Daarbij ziet het managementteam toe op de naleving van het betrokken beleid en rapporteert periodiek aan het bestuur over de realisatie en uitvoering van het bestuursbesluit.
Dit betekent onder andere:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor het Alma College
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten coördineren

Gegevensbescherming
De functionaris voor gegevensbescherming (FG) houdt binnen het Alma 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 (bestuur). De FG heeft regelmatig overleg met de verantwoordelijke IBP. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Informatiebeveiliging
Het managementteam heeft, naast de rol verantwoordelijkheid IBP, de rol informatiebeveiliging (ICT, privacy) in de portefeuille.

Security Team (ST)
Het Security Team vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Functioneel/Applicatiebeheer
Ieder softwarepakket of (web-)applicatie wordt beheerd door het functioneel/applicatiebeheer. Bij vragen over de software of applicatie is dit beheer het aanspreekpunt. Het beheer wordt door de eindverantwoordelijk schoolleider voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan worden de taken uitgevoerd.

Medewerkers
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging en privacy. Dit kan door meldingen te maken van security incidenten en datalekken, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).

Leidinggevenden
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 IBP-beleid;
- 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 personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de manager IBP. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

IBP team
Een IBP-team wordt organisatie breed zowel preventief als curatief benoemd voor informatiebeveiliging en privacy incidenten. De leden van het IBP-team zijn benoemd door het CvB en handelen in diens opdracht. Bij een calamiteit kan het IBP-team terstond bij elkaar worden geroepen op initiatief van de verantwoordelijke IBP. Het doel hiervan is om de continuïteit van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

- Beveiligingsincidenten en datalekken;
- Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
- Natuurrampen (brand, overstroming, storm, etc.).

Het IBP-team van het Alma College behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident. De werkzaamheden van het IBP-team van het Alma College zijn gedocumenteerd en door de eindverantwoordelijke bekrachtigd.