2023.245

Informatiebeveiligings- en privacybeleid

Minkema College

Formele versie gericht op accountability

Vastgesteld door het College van Bestuur van het Minkema College:

Versie	Datum	Naam	Functie
1.0	09-01-2019	Henk Heethuis	Directeur-bestuurder
2.0	18-12-2023	Mark de Haas	Vz College van Bestuur

Stichting Minkema College
Voor openbaar voortgezet onderwijs in Woerden en omstreken
Statutair gevestigd in Woerden

Bestuur nummer:	13360
BRIN-nummer:	17AN
Sector:	VO
Adres:	Minkemalaan 1 3446 GL Woerden
Telefoon:	0348 484 100
Email:	post@minkema.nl
Website:	www.minkema.nl
Contactpersoon:	B. Elemans, directeur bedrijfsvoering
Email:	b.elemans@minkema.nl

Inhoudsopgave

1 Het belang van informatiebeveiliging en privacy en de privacy-missie van het Minkema College

1.1 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. 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.

1.2 De privacymissie van het Minkema College

Het Minkema College heeft als vertrekpunt voor zijn privacybeleid de volgende privacymissie geformuleerd:

Het Minkema College behandelt zijn leerlingen, medewerkers en relaties met respect. Het Minkema College gaat daarom integer, transparant en zorgvuldig om met persoonsgegevens en verwerkt deze in overeenstemming met wet- en regelgeving op het gebied van de bescherming van Persoonsgegevens, zoals de Algemene Verordening Gegevensbescherming (AVG).

2 Toelichting informatiebeveiliging en privacy

2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een aantal 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 de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

Uit oogpunt van de kwaliteit van de informatievoorziening, hecht het Minkema College er daarnaast waarde aan dat de informatie in zijn systemen en bestanden steeds zo *actueel* mogelijk is.

2.2 Toelichting privacy

Privacy gaat o.a. 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 waarmee een natuurlijke persoon direct of indirect geïdentificeerd kunnen worden. Onder

verwerken wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerken:
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

Informatiebeveiliging en de bescherming van persoonsgegevens zijn nauw met elkaar verbonden en worden daarom samengevoegd in één organisatieproces, informatiebeveiliging en privacy; hierna verder afgekort tot IBP. Het is dan ook logisch hiervoor een samenhangend beleid te formuleren en te hanteren. Wij noemen dit ons informatiebeveiligings- en privacybeleid (het IBP-beleid).
Dit beleid vormt als het ware de kapstok voor de verdere uitwerking van richtlijnen, procedures en protocollen.

3 Doelen, reikwijdte en uitgangspunten van het informatiebeveiligings- en privacy beleid

3.1 Doelen

Het IBP-beleid van het Minkema College heeft de volgende doelen:

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

3.2 Reikwijdte

- Het IBP-beleid geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices waarmee geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen het Minkema College waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan het Minkema College persoonsgegevens verwerkt.

- Het IBP-beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het Minkema College. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en in beginsel ook niet-gecontroleerde informatie waarop de school kan worden aangesproken.

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

3.3 Uitgangspunten

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

1. Het Minkema College streeft naar een juiste balans tussen privacy, functionaliteit en veiligheid. In overeenstemming met de hiervoor geformuleerde privacymissie, is een belangrijk vertrekpunt daarbij altijd dat de persoonlijke levenssfeer van de betrokkenen wordt gerespecteerd en dat het Minkema College voldoet aan alle relevante wet- en regelgeving.

2. Als verwerking verantwoordelijke in de zin van de wet, neemt het College van Bestuur(hierna: CvB) van het Minkema College de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy afdoende geregeld worden. Het CvB is hierop aan te spreken en legt hier verantwoording over af. Tegelijkertijd is binnen het Minkema College het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.

3. Het Minkema 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.

4. Het Minkema 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 voor de school en/of de betrokkenen. Het Minkema College heeft specifiek een gedragscode geformuleerd, vastgesteld en geïmplementeerd; de Minkema Code. Voor leerlingen geldt er binnen het Minkema College een leerlingenstatuut.

5. Informatiebeveiliging en privacy is bij het Minkema College een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is. Dit document wordt 3-jaarlijks herzien; de eerstvolgende keer derhalve in 2026.

4 Uitwerking van het beleid – het hoe en wat

Dit hoofdstuk geeft een praktische invulling van bovenstaande uitgangspunten en is daarmee de uitwerking van het IBP-beleid op hoofdlijnen.

4.1 Basisprincipes en gedragsregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de principes leidend, die door de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) zijn vastgelegd; de zgn. *Fair Information Principles*. Deze principes zijn ook het fundament van de nieuwe privacywetgeving, de AVG. Op basis hiervan gelden er voor het Minkema College samengevat de volgende **tien gedragsregels** met betrekking tot de omgang met persoonsgegevens:

1. Het Minkema College beperkt zich bij het verzamelen van persoonsgegevens tot enkel die gegevens die het op rechtmatige wijze en met redelijke middelen heeft verkregen en indien van toepassing altijd met kennis of toestemming van de betrokkenen.

2. Het Minkema College zorgt ervoor dat de door hem verzamelde persoonsgegevens beperkt blijven tot de doelen waarvoor ze worden verzameld en dat deze steeds juist, compleet en up-to-date zijn.

3. Het Minkema College verzamelt enkel persoonsgegevens nadat:
    a. de doelen van het verzamelen afdoende en op voorhand bekend zijn gemaakt;
    b. duidelijk is dat het gebruik beperkt wordt tot het realiseren van deze doelen; OF
    c. tot andere (van geval tot geval gespecificeerde) doelen die niet strijdig zijn met het doel waarvoor ze eerder werden verzameld.

4. Wij stellen geen persoonsgegevens ter beschikking voor andere doelen dan waarvoor ze zijn verzameld, behalve dan op grond van:
    a. expliciet door de betrokkene gegeven toestemming;
    b. een wettelijke verplichting

5. Het Minkema College zorgt ervoor dat de aan hem ter beschikking gestelde persoonsgegevens passend worden beveiligd tegen verlies, vernietiging, ongeautoriseerde toegang, ongeoorloofd gebruik, -veranderingen, of terbeschikkingstelling.

6. Het Minkema College communiceert actief op beide locaties over haar privacybeleid, met inbegrip van de aard en reden van de verwerking van persoonsgegevens en de rechten van betrokkenen.

7. Het Minkema College zorgt ervoor dat iedere persoon die zich bij de school meldt:
    a. antwoord krijgt op de vraag of wij persoonsgegevens over hem/haar hebben;
    b. de feitelijke beschikking krijgt over deze hem betreffende persoonsgegevens;
    c. deze gegevens in beginsel kosteloos en in een leesbare vorm krijgt;
    d. en indien hem/haar dit wordt geweigerd, dit onder vermelding van reden wordt geweigerd alsmede de wijze waarop hiertegen beroep kan worden aangetekend;
    e. de hem/haar betreffende persoonsgegevens kan aanvechten en -indien terecht- kan eisen dat deze persoonsgegevens worden verwijderd, gecorrigeerd, aangevuld of gewijzigd.

8. Het Minkema College zorgt ervoor dat het op ieder moment in staat is verantwoording af te leggen over de wijze waarop het als organisatie invulling geeft aan zijn privacygedragsregels.

9. Het Minkema College zorgt ervoor dat de door hem verzamelde persoonsgegevens niet langer worden bewaard dan nodig voor het realiseren van het/de op voorhand aangegeven doel(en) waarvoor ze zijn verzameld.

10. Het Minkema College draagt geen persoonsgegevens over naar een land of gebied buiten de EER landen, voordat het zich ervan heeft verzekerd dat het ontvangende land de rechten en vrijheden van betrokkenen, waar het de verwerking van persoonsgegevens betreft, afdoende waarborgt en beveiligt.

4.2 Ondersteunende richtlijnen, procedures en protocollen

Diverse richtlijnen, procedures en protocollen geven invulling aan het beleid. De meest actuele versies daarvan zijn gepubliceerd op het Intranet van het Minkema College. Bijlage 1 geeft een overzicht van de diverse documenten die reeds zijn gepubliceerd of nog in ontwikkeling zijn.

4.3 Verwerkingsregister

Het Minkema College legt alle verwerkingen van persoonsgegevens vast in een verwerkingsregister en zal dit up-to-date houden. Het Minkema College voldoet hiermee aan de documentatieplicht op grond van de AVG.

4.4 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 regelmatig aangescherpt, zodat de kennis van risico's bij het omgaan met persoonsgegevens wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en andere betrokkenen. Verhoging van het bewustzijn m.b.t informatiebeveiliging en privacy is een gezamenlijke verantwoordelijkheid van de directie verantwoordelijke voor het IBP-beleid, de afdeling ICT en de Functionaris Gegevensbescherming, met het CvB als eindverantwoordelijke.

4.5 Classificatie en risicoanalyse

Het Minkema College classificeert informatie en informatiesystemen waarop het IBP-beleid van toepassing is. Deze classificatie is het uitgangspunt voor de risicoanalyse van de veiligheid van informatie en persoonsgegevens en voor de te nemen beveiligingsmaatregelen.

Bij de classificatie zijn beschikbaarheid, integriteit en vertrouwelijkheid de aspecten die van belang zijn. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie.
Voorafgaand aan de start van nieuwe (ICT)projecten, zoals wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, en voorafgaand aan nieuwe verwerkingen wordt gekeken naar de impact op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden om risico's te voorkomen of beperken. Hierbij moet er altijd een gezonde balans zijn tussen de risico's die het Minkema College wil afdekken en de benodigde investeringen verbonden aan de te nemen maatregelen.

4.6 Afspraken met verwerkers

Het Minkema College sluit met alle leveranciers, waaronder die van digitale onderwijsmiddelen en bedrijfsapplicaties, verwerkers overeenkomsten af als zij in opdracht van de schoolpersoonsgegevens verwerken. In termen van de AVG geldt het Minkema College dan als verwerkingsverantwoordelijke en de leveranciers als verwerkers.

Bij het afsluiten van deze verwerkersovereenkomsten zijn de bepalingen van de meest recente versie van het 'Convenant Digitale onderwijsmiddelen en privacy' voor het Minkema College zoveel mogelijk leidend.

4.7 Incidenten en datalekken

Het Minkema College heeft een protocol voor de melding en afhandeling van beveiligingsincidenten en datalekken: Protocol informatiebeveiligingsincidenten en datalekken Minkema College Dit protocol omvat een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten moeten worden gemeld bij helpdesk@minkema.nl en worden vastgelegd in een incidentenregister.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

4.8 Planning en controle

Dit IBP-beleid wordt in beginsel elke drie jaar getoetst en zo nodig bijgesteld door het College van Bestuur. 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 Minkema 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.

4.9 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 gedragscode en met periodieke bewustwordingscampagnes.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het College van Bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.
Mocht de naleving van dit beleid ernstig tekortschieten, dan kan het College van Bestuur de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

4.10 Logging en monitoring

Logging en monitoring door de afdeling ICT 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. Daarnaast legt de afdeling ICT de incidenten die gemeld zijn vast in het register voor informatiebeveiligingsincidenten en datalekken. Zie hiervoor ook onder 4.7.

5 Organisatie - Wie doet wat?

5.1 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 speelt de verdeling van verantwoordelijkheden en taken en de samenwerkingsrelatie tussen de verschillende actoren (functies / rollen en afdelingen) binnen het Minkema College een belangrijke rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen binnen het Minkema College.

Niveau	**Richtinggevend (strategisch)**	
Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren van / vastleggen in**
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	• Informatiebeveiligings- en privacy beleid vaststellen • Basismaatregelen vaststellen • Reglement FG vaststellen • Privacyreglement vaststellen
Niveau	**Sturend (tactisch)**	
Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** Het realiseren van en vastleggen in processen, richtlijnen en procedures van:
Directie-verantwoordelijke voor IBP-beleid *Deze rol is bij het Minkema College belegd bij de Directeur Bedrijfsvoering (DB)*	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert CvB over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	• Activiteiten Kalender / Jaaragenda • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen

Functionaris voor Gegevensbescherming (FG)	• Toezicht en advisering op naleving privacy wetgeving • Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Waar nodig de Directieverantwoordelijke voor IBP-beleid adviseren en ondersteunen • Ondersteuning bij afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
Afdelingshoofden c.q. adviseurs van: Afdelingsleiders, Onderwijsonder-steuning, ICT, P&O, Facilitair en Financiën.	• Classificatie / risicoanalyse in samenwerking met DB voor IBP-beleid en de FG. • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door CvB • Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
Niveau	**Uitvoerend (operationeel)**	
Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren van / vastleggen in**
Medewerkers Helpdesk ICT	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures.	

Medewerker	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • 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 bestuur.	
Dagelijkse leiding / leidinggevende / directie	• 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.	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 overzicht van de binnen het Minkema College beschikbare, aanvullende richtlijnen, procedures en protocollen die relevant zijn voor naleving van wet- en regelgeving m.b.t. privacy.

Documenten / bestanden:	**Vindplaats:**
Privacyverklaring voor leerlingen	Privacyverklaring leerlingen
Privacyverklaring voor ouders /verzorgers	Privacyverklaring ouders
Privacyreglement (rechten betrokkenen)	Privacyreglement
Protocol informatiebeveiligingsincidenten en datalekken	Datalekprotocol
Procedure toestemming gebruik beeldmateriaal	Beschikbaar in toestemming module in Magister
Verwerkersovereenkomsten met leveranciers	Overzicht op aanvraag beschikbaar bij Inkoop en functionaris AVG
Verwerkingsregister	Samenvatting op aanvraag beschikbaar bij functionaris AVG
Bewaar- en verwijderbeleid persoonsgegevens	Beschikbaar in Magister
Social Media Protocol	Social media protocol
Reglement Cameratoezicht	Reglement Cameratoezicht

Bijlage 2: Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBP binnen het Minkema College op drie niveaus wordt georganiseerd.

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

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken, worden binnen het Minkema College voor elk niveau 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.

Richtinggevend

Het College van 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.

Sturend

De directieverantwoordelijke voor IBP-beleid is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur), bewaakt een goede uitvoering van het IBP-beleid en stuurt waar nodig bij. Hij/zij is verder verantwoordelijk voor:

- Het IBP-beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit van IBP bewaken binnen het Minkema College.
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen het Minkema 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 datalek-incidenten, adviseert over privacy-aangelegenheden, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het bestuur). De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Directeur Bedrijfsvoering

Hij adviseert het College van Bestuur en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen het Minkema College. Hij is verantwoordelijk voor het afhandelen van informatiebeveiligingsincidenten.

Afdelingsleiders/Adviseurs

Binnen de school zijn er verschillende domeinen en afdelingen, zoals havo, vwo, mavo, vmbo, P&O, Onderwijs ondersteuning, facilitair&ICT en financiële zaken. Op elk van deze afdelingen is de leidinggevende verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

De afdelingshoofden zijn tevens verantwoordelijk voor het voorkomen dat personen ten onrechte (te ruime) toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben afdelingshoofden de volgende specifieke taken:

- Samen met de directieverantwoordelijke voor IBP-beleid stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

Uitvoerend

ICT afdeling

De coördinator ICT vormt samen met zijn helpdesk-team een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Applicatie of functioneel beheerder

Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De functioneel beheerder wordt vanuit de haar of zijn leidinggevende zijnde afdelingsleider of adviseur, voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Medewerker

Alle medewerkers dragen verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. de Minkema Code en de privacy gedragsregels. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.
Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van informatiebeveiligingsincidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel, in afdelingsoverleg of via de MR)

Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering binnen het Minkema College. 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;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in deze taak ondersteund worden door de directieverantwoordelijke voor IBP-beleid en/of geadviseerd worden door de functionaris gegevensbescherming. Leidinggevenden hebben ook wat betreft IBP een voorbeeldrol ten opzichte van hun medewerkers.