

INFORMATIEBEVEILIGINGS- EN PRIVACY BELEID

Formele versie



Beleidsdocument IBP

© 2018 Schoolvereniging Rehoboth

Bron: saMBO-ICT
Kennisnet

Bewerkt: Schoolvereniging Rehoboth

Versie	Status	Datum	Auteur	Omschrijving
0.1	concept	1-3-2018	Catharinus Doornbos	

Vastgesteld door Schoolvereniging Rehoboth

Versie	Datum	Naam	Functie	Paraaf
1.0	10-04-2018	Wilma Dorleijn	Algemeen Directeur a.i.	
1.0	09-04-2018	Frits Cleveringa	Voorzitter GMR	

Inhoudsopgave

1	Inleiding	1
1.1	Toelichting informatiebeveiliging	1
1.2	Toelichting privacy	1
1.3	Vervlechting informatiebeveiliging en privacy	1
2	Doel en reikwijdte	2
2.1	Doel	2
2.2	Reikwijdte	2
3	Uitgangspunten	3
3.1	Algemene beleidsuitgangspunten	3
3.2	Uitgangspunten privacy	4
4	Wet- en regelgeving	4
5	Organisatie	5
5.1	Rollen (functies) rondom IBP	5
5.2	Richtinggevend	5
5.3	Sturend	5
5.4	Uitvoerend	6
6	Controle en rapportage	7
6.1	Voorlichting en bewustzijn	7
6.2	Classificatie en risicoanalyse	7
6.3	Incidenten en datalekken	7
6.4	Controle, naleving en sancties	8
BIJLAGEN:	9

Informatiebeveiligings- en Privacy Beleid

1 Inleiding

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ICT. Deze afhankelijkheid van ICT en gegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy (IBP) 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.

1.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.

Deze aspecten zijn:

- 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 onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van Schoolvereniging Rehoboth en haar scholen. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

1.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. 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.*

In het 'Privacyreglement persoonsgegevens' geven we weer, hoe we hier concreet mee om gaan.

1.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Het

onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen Schoolvereniging Rehoboth.

2 Doel en reikwijdte

2.1 Doel

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers en leerlingen, wordt gerespecteerd en Schoolvereniging Rehoboth voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen Schoolvereniging Rehoboth geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties, alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van Schoolvereniging Rehoboth. Het beleid heeft zowel betrekking op gecontroleerde als op niet-gecontroleerde informatie. Gecontroleerde informatie betreft informatie, die door de school zelf is gegenereerd en wordt beheerd. Niet-gecontroleerde informatie betreft informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites.
- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Schoolvereniging Rehoboth waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties, evenals op andere betrokkenen waarvan Schoolvereniging Rehoboth persoonsgegevens verwerkt.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde of systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van Schoolvereniging Rehoboth evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het 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 binnen Schoolvereniging Rehoboth heeft raakvlakken met:
 - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
 - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
 - IT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale)

- leermiddelen
- Medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers
- Beleid inzake aanschaf en gebruik van digitale leermiddelen

3 Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Schoolvereniging Rehoboth zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking treedt).
- De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van Schoolvereniging Rehoboth om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.
- Binnen Schoolvereniging Rehoboth 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 fysieke documenten.
- Schoolvereniging Rehoboth en onderliggende scholen zijn als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast behoren Schoolvereniging Rehoboth en onderliggende scholen informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij Schoolvereniging Rehoboth geclassificeerd. De classificatie is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik gemaakt wordt van de classificatie. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- Schoolvereniging Rehoboth sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen Schoolvereniging Rehoboth en/of onderliggende scholen. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant 'Digitale leermiddelen privacy' (www.privacyconvenant.nl) en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht 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 imagooverlies. Schoolvereniging Rehoboth heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

- Informatiebeveiliging en privacy is bij Schoolvereniging Rehoboth een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij Schoolvereniging Rehoboth vanaf de start rekening gehouden met informatiebeveiliging en privacy.

3.2 Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij Schoolvereniging Rehoboth zijn:

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 wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag:** verwerking van Persoonsgegevens is gebaseerd op een van de 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. 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 deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast 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.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van toestemming, zal door Schoolvereniging Rehoboth en onderliggende scholen aan de Betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

4 Wet- en regelgeving

Schoolvereniging Rehoboth voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet

- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 2.0' leidend bij het maken van afspraken met leveranciers.

5 Organisatie

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.

Dit hoofdstuk beschrijft hoe IBP binnen Schoolvereniging Rehoboth is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen

5.1 Rollen (functies) rondom IBP

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Schoolvereniging Rehoboth een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

5.2 Richtinggevend

Eindverantwoordelijke

De Algemeen Directeur 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 manager IBP.

5.3 Sturend

Functionaris voor Gegevensbescherming

De Functionaris voor Gegevensbescherming (FG) houdt binnen Schoolvereniging Rehoboth 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 afhandelen van vertrouwelijke informatiebeveiligingsincidenten. De FG is meestal ook de contactpersoon voor klachten en vragen van betrokkenen.

De Functionaris voor Gegevensbescherming heeft binnen Schoolvereniging Rehoboth tevens de rol van Manager IBP. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op uitvoerend niveau. De Manager IBP moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling.
- De uniformiteit bewaken binnen Schoolvereniging Rehoboth.
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy.
- De verdere afhandeling van incidenten binnen Schoolvereniging Rehoboth coördineren.

Domeinverantwoordelijke / proceseigenaar

Binnen de school zijn er verschillende domeinen/processen, zoals ICT, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

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

- Samen met de Algemeen Directeur stellen zij het beleid voor toegang vast.
- Samen met Bovenschools ICT-coördinator en de externe ICT-beheerder zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- Samen met Bovenschools ICT-coördinator en de externe ICT-beheerder beoordelen zij regelmatig de toegangsrechten van gebruikers.

Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

5.4 Uitvoerend

Bovenschools ICT-coördinator

De Bovenschools ICT-coördinator is als Security Officer en Functioneel Beheerder een technisch aanspreekpunt inzake informatiebeveiliging voor het management en de medewerkers. Hij/zij wordt vanuit de domeinverantwoordelijke / proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn helder voor hen beschreven. 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 security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR of GMR)

Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat de 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 personeel gerelateerde IBP-onderwerpen. De leidinggevende kan in zijn/haar taak ondersteund worden door de Functionaris voor Gegevensbescherming/Manager IBP.

6 Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door het Directieboard. Hierbij wordt rekening gehouden met:

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

Daarnaast kent Schoolvereniging Rehoboth 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.

Voor alle overlegmomenten geldt dat deze zoveel mogelijk ingepast worden in bestaande overlegvormen met hetzelfde karakter waarbij op:

- **strategisch** niveau richtinggevend wordt gesproken over organisatie en compliance, alsmede over doelen, scope en ambitie op het gebied van IBP.
- **tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **operationeel** niveau worden de onderwerpen besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd, en indien nodig in elk organisatieonderdeel van Schoolvereniging Rehoboth.

6.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij Schoolvereniging Rehoboth 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, externen en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP en Bovenschools ICT-coördinator met de Algemeen Directeur als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse

Bij Schoolvereniging Rehoboth heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de 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 kwaliteitsaspecten die van belang voor de informatievoorziening.

6.3 Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij de Manager IBP en de Bovenschools ICT-coördinator. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

6.4 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Schoolvereniging Rehoboth wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een verenigingsbrede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de Algemeen Directeur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door de Algemeen Directeur vast te stellen reglement.

Mocht de naleving ernstig tekort schieten, dan kan Schoolvereniging Rehoboth de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Bij Schoolvereniging Rehoboth is het melden van beveiligingsincidenten en datalekken vastgelegd in het Protocol IBP Incidenten en Datalekken.

BIJLAGEN:

Bijlage 1 – Rollen en Taken

Bijlage 2 – Classificatie Formulier

Bijlage 3 – Risico Analyse Formulier

Bijlage 4 – Overzicht Digitale Onderwijsmiddelen

Bijlage 5 – Reglement internet en sociale media

Bijlage 6 – Reglement ICT Middelen