SSBB
Stichting Scholen
met de Bijbel in
de Betuwe

AVG en privacy SSBB

1. Protocol datalekken
2. Privacy reglement
3. Privacyverklaring
4. Gedragscode ICT en internet
5. Reglement cameratoezicht
6. IBP beleid SSBB
7. Reglement FG

De GMR heeft op 15 april 2019 ingestemd met onderstaande documenten.

Inhoud

Protocol datalekken

Inleiding
Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken.
Dit protocol is van toepassing op alle scholen van Stichting Scholen met de Bijbel in de Betuwe, zoals vermeld in het IBP-beleid en al haar medewerkers.

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening;** het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de school.
- **Datalek;** een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene;** de persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken
Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn scholen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Vanaf 25 mei 2018 is dit opgenomen in de Algemene Verordening Persoonsgegevens (AVG). Het nalaten van deze melding kan leiden tot een fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in het leerlingadministratiesysteem, salarispakket, mail of digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze verwerkers aanvullende afspraken over het melden van datalekken.

Beveiligingsincident datalek
Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie ‘gelekt’.

Voorbeelden van beveiligingsincidenten zijn:
Verlies of diefstal van waardepapier, dossier, tablet of andere gegevensdragers
Niet naleven van beleid of richtlijnen
Inbreuk op fysieke beveiligingsvoorzieningen
Toegangsovertredingen
Opzettelijk foutief handelen (fraude, diefstal)
Beschadigen of vernielen van (kritische) apparatuur
Virusbesmetting als gevolg van het aanklikken van een onbetrouwbare bijlage
Onbevoegd inzien van vertrouwelijke informatie
Onbedoelde openbaarmaking van vertrouwelijke informatie
Geen gescreend personeel
Illegale licenties
Illegaal kopiëren van gegevens
Email met onversleutelde vertrouwelijke informatie

Kenbaar maken van of onzorgvuldig omgaan met wachtwoorden
Maar ook cyberaanvallen zoals een ddos, computerhacking of besmetting met ransomware , of het technische falen van apparatuur, stroomuitval, wateroverlast en dergelijke zijn aan te merken als incidenten.

Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid;
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen en/of gedragscode ict en internetgebruik.

De vier rollen

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1. **Ontdekker** (medewerker); degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.

1.1. **Ontdekker** (externe); een ouder of verwerker die een beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.

2. **Meldpunt** (Privacy Officer of Functionaris voor Gegevensbescherming); een aanspreekpunt binnen de school waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder** (Functionaris voor Gegevensbescherming); degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus** (Privacy Officer of externe ict-dienstverlener); degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is het toezichthoudend bestuur. Een leverancier is een verwerker voor de school. De FG doet in overleg met de verantwoordelijke (bestuurder) de melding De verwerker kan een melding doen, echter dit is dan afgesproken met de verantwoordelijke.

Als er een datalek is, moet daar **binnen 72 uur** na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

De stappen

Ontdekken

De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het Meldpunt via de Privacy Officer; privacy@ssbb.nl.

Inventariseren

Het Meldpunt bepaalt aan de hand van een formulier of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt in het formulier vastgelegd:
Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
Datum/periode van het beveiligingsincident
Aard van het beveiligingsincident
Wanneer van toepassing (bij een datalek):
Omschrijving van de groep betrokkene
Aantal betrokkene

Type persoonsgegevens in kwestie
Worden de gegevens binnen een keten gedeeld

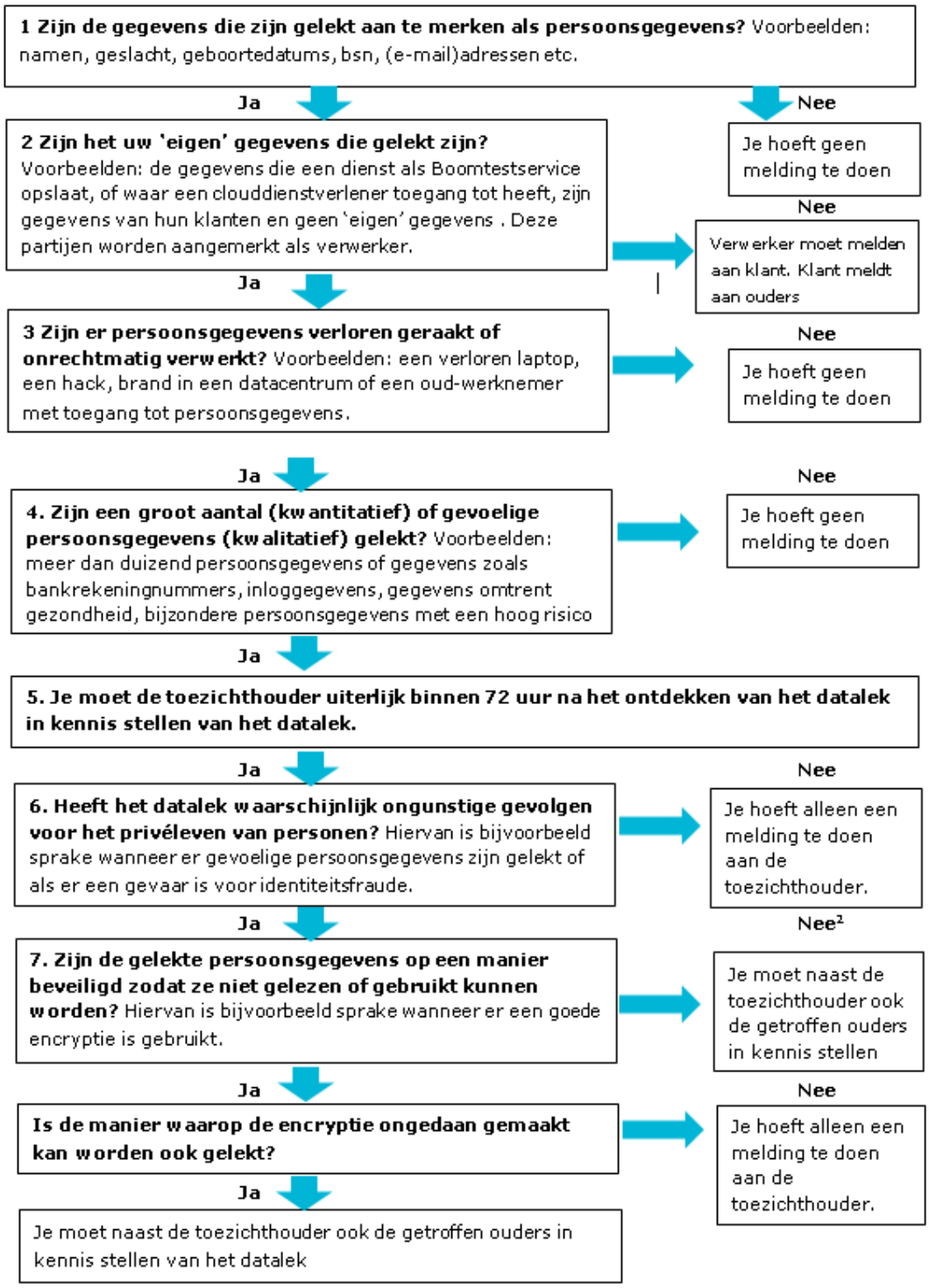
Beoordelen
Wanneer het Meldpunt (Privacy Officer) voldoende informatie heeft verzameld, en een datalek vermoedt, stuurt deze de Functionaris voor Gegevensbescherming (FG) een verzoek om de verzamelde informatie te bekijken. De FG beoordeelt de feiten om te bepalen of een melding aan de Autoriteit Persoonsgegevens en/of betrokkene vereist is.

De volgende informatie wordt vastgelegd door de Functionaris voor Gegevensbescherming (FG):
Impact van de melding
Welk type gegevens er verloren gegaan zijn
Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkene
Aard van de inbreuk
Gaat het om gegevens die uitbesteed zijn aan een verwerker
Aantal betrokkenen
Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
Wordt het datalek aan betrokkene gemeld? Waarom niet?
Hoe worden meldingen gedaan? Wat is de inhoud van de melding?
Wordt er melding gedaan via de Pers?

Bij de beoordeling of er sprake is van een ‘meldingsplichtig datalek’, wordt er rekening gehouden met het type gegevens, en met de hoeveelheid gegevens.
Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, **moet** er gemeld worden.
Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens ‘gevoelig’ zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene.

Jaarlijks worden zowel het toezichthoudend bestuur als de GMR ingelicht over het aantal meldingen en de genomen maatregelen. Indien er sprake is van een ernstig en of ‘groot’ datalek zal het toezichthoudend bestuur en de GMR eerder ingelicht worden.

De beslisboom op de volgende pagina kan worden gebruikt:



Repareren

De Privacy Officer wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De Privacy Officer legt onderstaande vast:

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
- Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

Herstelaanpak datalekken

Bij de herstelaanpak wordt rekening gehouden met de volgende twee vragen:

- Hoe herstel je de schade bij betrokkene?
  - Wat kun je doen om betrokkenen te ondersteunen in het beperken van de schade door een datalek?
  - Op welke wijze ga je deze nazorg leveren?
  - Wie worden hierbij betrokken? *(denk aan marketing, leverancier, bestuurder, HRM)*
- Hoe herstel van de schade van de school?
  - Op welke wijze kan de schade van de school beperkt blijven dan wel hersteld worden?
  - Wie worden hierbij betrokken? *(marketing/communicatie, leverancier, MT en bestuurder, HRM)*
  - Maakt het datalek de uitvoering van een bedrijfsproces onmogelijk en bestaat daarvoor een alternatieve werkwijze?
  - Wat voor acties ga je ondernemen om de reputatieschade te beperken en om de reputatie te herstellen?
  - Wat voor acties ga je ondernemen rondom de afwikkeling van aansprakelijkheidsstelling en boetes?
  - Welke acties worden ondernomen ter voorkomen en communicatie aan medewerkers?

Melden

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Functionaris voor Gegevensbescherming (FG) dit binnen 72 uur in overleg met de bestuurder doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de Functionaris voor Gegevensbescherming (FG) waarmee het incident is afgesloten. De FG verstuurt een samenvatting van de genomen maatregelen aan de Privacy Officer en deze stuurt door naar de Ontdekker.

Informeren betrokkene

Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkene zelf worden gemeld. Dat zijn medewerkers en leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan ervan worden uitgaan dat lekken van gevoelige aard gemeld moeten worden bij de betrokkene.

Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkene te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Stappenplan
Onderstaande stappen wordt gebruikt voor communicatie naar de medewerkers.

	Procedurestap	Termijn	Wie
1	**Beveiligingsincident** • Verlies iPad, smartphone, laptop • Verzending naar verkeerd mailadres • Verlies dossier • Onbevoegde die toegang had tot netwerk of bestand • Phishing • Hacking		Ontdekker lek
1	**Beveiligingsincident** melden bij Privacy Officer en direct leidinggevende **privacy@ssbb.nl**	Direct	Ontdekker lek
1a	Indien telefoon verloren etc. direct gaan blokkeren (ook privé telefoon)	Direct	Privacy Officer
1b	Ook persoonsgegevens gelekt? Dan ook melden bij functionaris gegevensbescherming (FG) **FG:** Stijn Sarneel; fg@lumengroup.nl	Direct	Privacy Officer
2	In behandeling nemen beveiligingsincident	Direct	FG
3	Maatregelen treffen om datalek te stoppen	Direct	Privacy Officer i.o.m. FG
3a	Informeren bestuurder over datalek	Direct	Directie/PO
4	Beoordelen of er sprake is van een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) Of er sprake is van een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) Of betrokkene(n) wiens gegevens gelekt zijn geïnformeerd moet(en) worden Of er actie ondernomen moet worden naar derden: Informatie Maatregelen Onderzoek Of de RvT e/o GMR geïnformeerd moeten worden Of externe communicatie nodig is	Binnen 72 uur na ont-dekken van lek	FG in overleg met: PO Medewerker /team dat gegevens verwerkt Direct leidinggevende Directeur-bestuurder
5	Informeren bestuurder over stand van zaken en beoordeling	Binnen 72 uur	Directie / PO
6	Bij meldingsplichtig datalek: melden bij AP via meldloket: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0	Binnen 72 uur	PO – voor verzenden overleg FG
7	Als betrokkene(n) wiens gegevens gelekt zijn geïnformeerd moet(en) worden, versturen kennisgeving met vermelding van: • Aard inbreuk • Contactgegevens • De maatregelen die betrokkene kan nemen om negatieve gevolgen te beperken Afhankelijk van de omvang van het datalek overwegen om andere kanalen in te zetten.	Zo snel mogelijk, uiterlijk binnen 72 uur	Directie/PO in overleg met medewerker / directeur die gegevens verwerkt FG in overleg met bestuurder

7a	Externe communicatie (indien nodig)	Zo snel mogelijk	Directeur-bestuurder/team dat gegevens verwerkt /FG
7b	Controle op effectiviteit van de afhandeling van incidenten en datalekken per kwartaal	FG	Per kwartaal
7c	Jaarlijkse rapportage over aantal datalekken aan RvT en GMR	Per jaar	PO en FG iom directeur-bestuurder

Privacyreglement

Bron
Kennisnet

Bewerkt door:
Stichting Scholen met de Bijbel in de Betuwe,

Versie	Status	Datum	Auteur	Omschrijving
0.1	Definitief	09-11-2018	Kennisnet en bewerkt door CED Marion ter Horst	

Vastgesteld door Stichting Scholen met de Bijbel in de Betuwe:

Versie	Datum	Naam	Functie
1.0	November 2018	M.J. van der Mark	Gemandateerd bestuurder

Privacyreglement voor Stichting Scholen met de Bijbel in de Betuwe

1. Toepasselijkheid	Dit reglement geldt voor de gehele organisatie die deel uitmaakt van Stichting Scholen met de Bijbel in de Betuwe. Stichting Scholen met de Bijbel in de Betuwe is gevestigd aan de Rembrandt van Rijnstraat 33 te Lienden.
2. Definities	
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‘de betrokkene’), zoals bijvoorbeeld naam, adres, geboortedatum, titel(s), geslacht, adres, telefoonnummer, e-mailadres, functie, personeelsnummer, medische rapportages, inhoud van e-mails, prestaties/cijfers, brieven, klachten, foto’s, video’s, IP-adressen, tracking cookies, loginnamen en wachtwoorden.
Verwerking van persoonsgegevens	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, geautomatiseerd of handmatig, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Bijzondere persoons-gegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische gegevens (DNA/RNA) of biometrische gegevens (bijv. foto’s) met het oog op de unieke identificatie van een persoon, en gegevens over gezondheid, of iemands seksueel gedrag of seksuele gerichtheid.
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft, en die al dan niet wordt vertegenwoordigd door een wettelijk vertegenwoordiger. Betrokkenen kunnen bijvoorbeeld zijn: leerlingen, ouders, medewerkers en bezoekers.
Wettelijk vertegenwoordiger	Degene die het ouderlijk gezag over een minderjarige uitoefent. Meestal zal dit een ouder zijn, maar het kan ook gaan om een voogd. Als een leerling 16 jaar of ouder is, beslist hij in voorkomende gevallen zelf over zijn privacy.
Verwerkingsverant-woordelijke	De entiteit die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit reglement is het bevoegd gezag, te weten Stichting Scholen met de Bijbel in de Betuwe, vertegenwoordigd door het toezichthoudend bestuur, de verwerkingsverantwoordelijke.
Verwerker	De natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke (Stichting Scholen met de Bijbel in de Betuwe) persoonsgegevens verwerkt, zoals bijvoorbeeld de leverancier van een leerlingvolgsysteem of leerling-administratiesysteem. Een verwerker heeft een uitvoerende taak, ten behoeve van de activiteiten van de verwerkingsverantwoordelijke.

Derde

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, de verwerkingsverantwoordelijke, de verwerker, of de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken.

BEVOEGD GEZAG

Stichting Scholen met de Bijbel in de Betuwe, de verwerkingsverantwoordelijke in de zin van dit reglement.

3. Reikwijdte en doelstelling

1. Dit reglement stelt regels over de verwerking van persoonsgegevens van alle betrokkenen bij de organisatie, waaronder leerlingen en hun wettelijk vertegenwoordigers, medewerkers, bezoekers en externe relaties (bijv. leveranciers en opdrachtnemers).
2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door de Stichting Scholen met de Bijbel in de Betuwe worden verwerkt. Het reglement heeft tot doel:

a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens;
b. vast te stellen met welk doel en op welke (juridische) grondslag persoonsgegevens binnen Stichting Scholen met de Bijbel in de Betuwe worden verwerkt;
c. ook overigens te borgen dat persoonsgegevens binnen Stichting Scholen met de Bijbel in de Betuwe rechtmatig, transparant en behoorlijk worden verwerkt;
d. de rechten van betrokkenen vast te leggen en te borgen dat deze rechten door Stichting Scholen met de Bijbel in de Betuwe worden gerespecteerd.

4. Doelen van de verwerking van persoonsgegevens

Bij de verwerking van persoonsgegevens houdt Stichting Scholen met de Bijbel in de Betuwe zich aan de relevante wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG), de uitvoeringswet AVG en de onderwijswetgeving.

Doelen

1. De verwerking van persoonsgegevens vindt plaats voor:
   a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, het voorzien in hun (extra) ondersteuningsbehoefte, dan wel het geven van studieadviezen;
   b. het verstrekken en/of ter beschikking stellen van leermiddelen;
   c. het bewaken van de veiligheid binnen de scholen en het beschermen van eigendommen van medewerkers, leerlingen en bezoekers;
   d. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld, onder a en b, alsmede van informatie over de leerlingen op de eigen website;
   e. het bekend maken van de activiteiten van de organisatie, bijvoorbeeld op de website van Stichting Scholen met de Bijbel in de Betuwe of van de scholen, in brochures of de schoolgids of via social media;
   f. het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen;

g. het aanvragen van bekostiging, het behandelen van geschillen daarover en het doen uitoefenen van accountantscontrole;
h. het onderhouden van contacten met oud-leerlingen;
i. het aangaan en uitvoeren van arbeidsovereenkomsten, samenwerkingsrelaties met opdrachtnemers en contracten met leveranciers;
j. de uitvoering of toepassing van wet- en regelgeving;
k. juridische procedures waarbij Stichting Scholen met de Bijbel in de Betuwe betrokken is.

2. De verwerking van persoonsgegevens mag ook plaatsvinden voor doelen die verenigbaar zijn met de doelen zoals beschreven in lid 1.

5. Doelbinding

Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. Stichting Scholen met de Bijbel in de Betuwe verwerkt niet meer gegevens dan noodzakelijk is om de betreffende doelen te bereiken.

6. Soorten persoonsgegevens

De categorieën van persoonsgegevens zoals deze binnen Stichting Scholen met de Bijbel in de Betuwe worden verwerkt, worden geregistreerd in een verwerkingsregister.

7. Grondslag verwerking

Verwerking van persoonsgegevens gebeurt alleen indien aan een van de onderstaande voorwaarden is voldaan:

a. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan Stichting Scholen met de Bijbel in de Betuwe is opgedragen.
b. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op Stichting Scholen met de Bijbel in de Betuwe rust.
c. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de arbeidsovereenkomst) of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.
d. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van Stichting Scholen met de Bijbel in de Betuwe of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen, met name wanneer de betrokkene een kind is; in het kader van deze grondslag zal dus een belangenafweging moeten plaatsvinden.
e. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen (levensbelang).
f. De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.

8. Bewaartermijnen

Stichting Scholen met de Bijbel in de Betuwe bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor deze worden verwerkt, tenzij het langer bewaren van de persoonsgegevens op grond van wet- of regelgeving verplicht is. Zie voor de bewaartermijnen bijlage 4.

9. Toegang

Binnen de organisatie van Stichting Scholen met de Bijbel in de Betuwe geldt dat personen slechts toegang hebben tot persoonsgegevens voor zover dat daadwerkelijk nodig is. De toegang van medewerkers tot persoonsgegevens is dan ook beperkt tot de gegevens die noodzakelijk zijn voor de goede uitoefening van hun functie en (dus) hun werkzaamheden. Verder wordt slechts toegang verschaft tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan:

a. de verwerker die van Stichting Scholen met de Bijbel in de Betuwe de opdracht heeft gekregen om persoonsgegevens te verwerken, maar alleen voor zover dat noodzakelijk is in het licht van de gemaakte afspraken;
b. derden voor zover uit de wet voortvloeit dat Stichting Scholen met de Bijbel in de Betuwe verplicht is om toegang te geven of sprake is van een (andere) grondslag voor deze verwerking, bijvoorbeeld de vervulling van een taak van algemeen belang.

10. Beveiliging en geheimhouding

1. Stichting Scholen met de Bijbel in de Betuwe neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. Deze maatregelen zijn er mede op gericht om niet noodzakelijke verzameling en verdere (niet noodzakelijke) verwerking van persoonsgegevens te voorkomen.
2. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen.
3. Een ieder die betrokken is bij de verwerking van persoonsgegevens binnen Stichting Scholen met de Bijbel in de Betuwe is verplicht tot geheimhouding van de betreffende persoonsgegevens, en zal deze gegevens slechts verwerken voor zover dat noodzakelijk is voor de uitoefening van de betreffende functie, werkzaamheden of taak.

11. Verstrekken gegevens aan derden

Stichting Scholen met de Bijbel in de Betuwe kan persoonsgegevens aan derden verstrekken als daarvoor een grondslag bestaat in de zin van artikel 7 van dit reglement.

12. Sociale media

Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het sociale mediaprotocol van Stichting Scholen met de Bijbel in de Betuwe.

13. Rechten betrokkenen

1. Stichting Scholen met de Bijbel in de Betuwe erkent de rechten van betrokkenen, handelt daarmee in overeenstemming en bewerkstelligt dat betrokkenen deze rechten daadwerkelijk kunnen uitoefenen. Het betreft in het bijzonder de volgende rechten:

Inzage

a. Een betrokkene heeft recht op inzage van de door Stichting Scholen met de Bijbel in de Betuwe verwerkte persoonsgegevens die op hem betrekking hebben, behalve voor zover het gaat om werkdocumenten, interne notities en andere documenten die uitsluitend bedoeld zijn voor intern overleg en beraad. Indien en voor zover dit recht op inzage ook de rechten en vrijheden

van anderen raakt, bijvoorbeeld als in de documenten ook persoonsgegevens van anderen dan de betrokkene zijn vermeld, kan Stichting Scholen met de Bijbel in de Betuwe het recht op inzage beperken.

Bij het verstrekken van de betreffende gegevens verschaft Stichting Scholen met de Bijbel in de Betuwe voorts informatie over:

- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens die worden verwerkt;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- (indien van toepassing) ontvangers in derde landen of internationale organisaties;
- (indien mogelijk) hoe lang de gegevens worden bewaard;
- dat de betrokkene het recht heeft om te verzoeken dat de persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van de persoonsgegevens wordt beperkt, alsmede dat hij het recht heeft om bezwaar te maken tegen de verwerking van de persoonsgegevens;
- het feit dat de betrokkene een klacht kan indienen bij de Autoriteit Persoonsgegevens;
- de bron van de persoonsgegevens, indien de persoonsgegevens niet van de betrokkene zelf zijn verkregen;
- het eventueel toepassen van geautomatiseerde besluitvorming en de betreffende onderliggende logica en het belang en de gevolgen voor de betrokkene;
- de passende waarborgen indien de persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie.

Verbetering, aanvulling, verwijdering

b. Stichting Scholen met de Bijbel in de Betuwe verbetert de persoonsgegevens van een betrokkene in het geval de betrokkene terecht heeft aangegeven dat de gegevens onjuist zijn, en Stichting Scholen met de Bijbel in de Betuwe vult de persoonsgegevens van een betrokkene aan indien de betrokkene terecht om aanvulling heeft verzocht. Voorts kan de betrokkene verzoeken om verwijdering van zijn persoonsgegevens. Stichting Scholen met de Bijbel in de Betuwe gaat daartoe over indien is voldaan aan een wettelijke grondslag voor het verzoek, tenzij het onmogelijk is om aan het verzoek te voldoen of dit een onredelijke inspanning zou vergen.

Bezwaar

c. Indien Stichting Scholen met de Bijbel in de Betuwe persoonsgegevens verwerkt op de grondslag van artikel 7 onder a of artikel 7 onder d van dit reglement, kan de betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens. In dat geval staakt Stichting Scholen met de Bijbel in de Betuwe de verwerking van de betreffende persoonsgegevens, behalve als naar het oordeel van Stichting Scholen met de Bijbel in de Betuwe het belang van Stichting Scholen met de Bijbel in de Betuwe, het belang van derden of het algemeen belang in het betreffende concrete geval zwaarder weegt.

Beperken verwerking

d. De betrokkene kan voorts verzoeken om de verwerking van zijn persoonsgegevens te beperken, namelijk indien hij een verzoek tot verbetering heeft gedaan, indien hij bezwaar heeft gemaakt tegen de verwerking, als de persoonsgegevens niet meer nodig zijn voor het doel van de verwerking of als de gegevensverwerking onrechtmatig is. Stichting Scholen met de Bijbel in de Betuwe staakt dan de verwerking, tenzij de betrokkene toestemming heeft gegeven voor de verwerking, Stichting Scholen met de Bijbel in de Betuwe de gegevens nodig heeft voor een rechtszaak of de verwerking nodig is ter bescherming van de rechten van een andere persoon of vanwege gewichtige redenen.

Kennisgevingsplicht

e. Als Stichting Scholen met de Bijbel in de Betuwe op verzoek van een betrokkene een verbetering of verwijdering van persoonsgegevens heeft uitgevoerd, of de verwerking van persoonsgegevens heeft beperkt, zal Stichting Scholen met de Bijbel in de Betuwe eventuele ontvangers van de betreffende persoonsgegevens daarover informeren.

Procedure

2. Stichting Scholen met de Bijbel in de Betuwe handelt een verzoek van een betrokkene zo spoedig mogelijk, maar uiterlijk binnen een maand na ontvangst van het verzoek, af. Afhankelijk van de complexiteit en van het aantal verzoeken kan die termijn indien nodig met twee maanden worden verlengd. Als deze verlenging plaatsvindt, wordt de betrokkene daarover binnen een maand na de ontvangst van het verzoek geïnformeerd. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt. Wanneer Stichting Scholen met de Bijbel in de Betuwe geen gevolg geeft aan het verzoek van de betrokkene, deelt Stichting Scholen met de Bijbel in de Betuwe onverwijld en uiterlijk binnen een maand na ontvangst mede waarom het verzoek niet wordt ingewilligd en informeert hij de betrokkene over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of beroep bij de rechter in te stellen.

Intrekken toestemming

3. Indien voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijde door de betrokkene of zijn wettelijk vertegenwoordiger worden ingetrokken. Als de toestemming wordt ingetrokken, staakt Stichting Scholen met de Bijbel in de Betuwe de verwerking van persoonsgegevens, behalve als er een andere grondslag (zoals bedoeld in artikel 7) voor de gegevensverwerking is. Het intrekken van de toestemming tast de rechtmatigheid van verwerkingen die reeds hebben plaatsgevonden niet aan.

14. Transparantie

Stichting Scholen met de Bijbel in de Betuwe informeert de betrokkene(n) actief over de verwerking van hun persoonsgegevens, in ieder geval door middel van een laagdrempelige privacyverklaring. In de privacyverklaring wordt in ieder geval de volgende informatie vermeld:

a. de contactgegevens van Stichting Scholen met de Bijbel in de Betuwe;

b. de contactgegevens van de functionaris voor gegevensbescherming van Stichting Scholen met de Bijbel in de Betuwe
c. de doeleinden van de gegevensverwerking en de grondslagen voor de verwerking;
d. een omschrijving van de belangen van Stichting Scholen met de Bijbel in de Betuwe indien de verwerking wordt gebaseerd op het gerechtvaardigd belang van Stichting Scholen met de Bijbel in de Betuwe;
e. de (categorieën) ontvangers van de persoonsgegevens, zoals verwerkers of derden;
f. in voorkomend geval: of de persoonsgegevens worden verzonden aan landen buiten de Europese Economische Ruimte (EER);
g. hoe lang de persoonsgegevens zullen worden bewaard;
h. dat de betrokkene het recht heeft om Stichting Scholen met de Bijbel in de Betuwe te verzoeken om inzage, verbetering of verwijdering van persoonsgegevens, en dat hij het recht heeft om te verzoeken om beperking van de verwerking, om bezwaar te maken of om een beroep te doen op het recht van gegevensoverdraagbaarheid;
i. dat de betrokkene het recht heeft om zijn toestemming in te trekken, als de gegevensverwerking is gebaseerd op toestemming;
j. dat de betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
k. of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te kunnen sluiten, en of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de gevolgen zijn indien hij de persoonsgegevens niet verstrekt;
l. het bestaan van geautomatiseerde besluitvorming, vergezeld van nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

15. Meldplicht datalekken

Een ieder die betrokken is bij een verwerking van persoonsgegevens is verplicht om een datalek per ommegaande te melden bij het meldpunt (privacy@ssbb.nl), conform het protocol beveiligingsincidenten en datalekken van Stichting Scholen met de Bijbel in de Betuwe. Een datalek is elke inbreuk waarbij persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk zijn gemaakt.

16. Klachten

a. Wanneer een betrokkene van mening is dat het doen of nalaten van Stichting Scholen met de Bijbel in de Betuwe niet in overeenstemming is met de AVG, dit reglement of (andere) toepasselijke wet- of regelgeving, dan kan een klacht worden ingediend overeenkomstig de binnen Stichting Scholen met de Bijbel in de Betuwe geldende klachtenregeling. Een betrokkene kan zich eveneens wenden tot de functionaris voor gegevensbescherming van Stichting Scholen met de Bijbel in de Betuwe (stijn.sarneel@lumengroup.nl)

b. Als een klacht naar de mening van betrokkene door Stichting Scholen met de Bijbel in de Betuwe niet correct is afgewikkeld, kan hij zich wenden tot de rechter of de Autoriteit Persoonsgegevens.

17. Onvoorziene situatie

Indien zich een situatie voordoet die niet beschreven is in dit reglement, neemt het toezichthoudend bestuur van Stichting Scholen met de Bijbel in de Betuwe de benodigde maatregelen, en wordt beoordeeld of dit reglement dientengevolge moet worden aangevuld of aangepast.

18. Wijzigingen reglement

1. Dit reglement is na instemming van de Gemeenschappelijke Medezeggenschapsraad (GMR) vastgesteld door het toezichthoudend bestuur van Stichting Scholen met de Bijbel in de Betuwe. Het reglement wordt gepubliceerd op de website van Stichting Scholen met de Bijbel in de Betuwe en de websites van de scholen. Het reglement wordt verder actief onder de aandacht gebracht, bijvoorbeeld door middel van verwijzing in de schoolgids.
2. Het toezichthoudend bestuur kan dit reglement wijzigen na instemming van de GMR.

19. Slotbepaling

Dit reglement wordt aangehaald als het privacyreglement van Stichting Scholen met de Bijbel in de Betuwe en treedt in werking in april 2019**.**

Privacyverklaring

Privacyverklaring; Hoe gaat Stichting Scholen met de Bijbel in de Betuwe om met persoonsgegevens.

Contactgegevens Stichting Scholen met de Bijbel in de Betuwe: Rembrandt van Rijnstraat, 4033 GH Lienden
Verwerkingsverantwoordelijke (bestuurder) van de school: de heer M.J. van der Mark
Contactgegevens Functionaris voor Gegevensbescherming:
de heer S. Sarneel
Tel: 06-51254290
stijn.sarneel@lumengroup.nl

Stichting Scholen met de Bijbel in de Betuwe verwerkt van al zijn leerlingen persoonsgegevens. Stichting Scholen met de Bijbel in de Betuwe vindt een goede omgang met persoonsgegevens van groot belang en is zich bewust van de privacywetgeving. Stichting Scholen met de Bijbel in de Betuwe is verantwoordelijk voor het zorgvuldig omgaan met de persoonsgegevens van uw kind. In deze privacy toelichting leggen wij u graag uit hoe wij met de persoonsgegevens van uw kind omgaan.

Waarom verwerken wij gegevens van uw kind

Stichting Scholen met de Bijbel in de Betuwe verwerkt persoonsgegevens van uw kind om onze verplichtingen als onderwijsinstelling te kunnen nakomen. Zo hebben wij bijvoorbeeld de gegevens nodig om uw kind aan te melden als leerling op onze school, om de studievoortgang bij te houden en om uw kind in staat te stellen een diploma te halen. Daarnaast hebben wij de wettelijke verplichting om bepaalde gegevens door te sturen naar andere partijen, zoals DUO (ministerie van Onderwijs) en leerplicht.
Wij verwerken gegevens van uw kind voor het uitvoeren van de onderwijsovereenkomst die we met uw kind hebben en/of voor het nakomen van onze wettelijke verplichtingen.
Gegevens die hier niet aan voldoen zullen wij alleen met uw toestemming verwerken. Als voor het verwerken van gegevens toestemming wordt gevraagd zoals voor het gebruik van beeldmateriaal (foto's en video's) dan kunt u de toestemming op elk moment intrekken of alsnog geven. (Wijziging van toestemming is niet van toepassing op inmiddels gepubliceerd beeldmateriaal).

Welke gegevens verwerken wij van uw kind

Wij verwerken diverse soorten gegevens, waarvan wij de meeste gegevens rechtstreeks van u als ouders hebben gekregen. U kunt hierbij denken aan contactgegevens en geboorteplaats. Als u weigert de voor ons noodzakelijke gegevens te verstrekken, kunnen wij onze verplichtingen niet nakomen. De verstrekking van deze gegevens is dan ook een voorwaarde om uw kind in te kunnen schrijven bij Stichting Scholen met de Bijbel in de Betuwe.

Welke persoonsgegevens wij van uw kind verwerken kun u terugvinden onderaan deze toelichting bij *Categorieën van persoonsgegevens*.
Op uw eigen verzoek en met uw uitdrukkelijke toestemming verwerken wij ook medische gegevens van uw kind. Dit beperkt zich enkel tot gegevens die nodig zijn om in noodgevallen goed te kunnen handelen. U kunt bijvoorbeeld doorgeven dat uw kind epilepsie heeft, zodat wij adequaat kunnen optreden in noodsituaties. Stichting Scholen met de Bijbel in de Betuwe zal u nooit dwingen dergelijke gegevens te overleggen.

Hoe gaan wij om met de gegevens van uw kind

Bij het verwerken van de gegevens gaan wij altijd uit van noodzakelijkheid, wij zullen niet meer gegevens verwerken dan noodzakelijk is om onze rechten en plichten als onderwijsinstelling na te komen. Dit betekent ook dat de gegevens niet zullen gebruiken voor andere doeleinden dan wij in deze toelichting noemen.

In een aantal gevallen zijn wij, zoals eerder aangegeven, verplicht om gegevens van uw kind te delen met andere organisaties. Dit zijn onder andere DUO, leerplicht, de onderwijsinspectie, GGD/schoolarts, samenwerkingsverband en accountant.

Wij kunnen commerciële derde partijen verzoeken om te ondersteunen bij het verwerken van de gegevens voor de eerder genoemde doeleinden. Denk hierbij aan applicaties om leerlingen in de les te ondersteunen, een administratie systeem waarbij de gegevens niet op ons eigen netwerk worden opgeslagen, maar bij een andere organisatie of een lesroosterprogramma. Dit gebeurt altijd in opdracht en onder de verantwoordelijkheid van Stichting Scholen met de Bijbel in de Betuwe. Met deze organisaties sluiten we overeenkomsten af, waarin o.a. is vastgelegd welke gegevens er verwerkt worden en hoe deze gegevens beveiligd worden.
Wij zullen de gegevens van uw kind niet delen met commerciële derde partijen voor andere doeleinden. Ook zullen wij de gegevens van uw kind nooit verkopen of verhuren aan derde partijen.

De persoonsgegevens worden zoveel mogelijk gecodeerd bewaard en alleen die medewerkers kunnen bij de gegevens, die dat ook voor de uitvoering van hun werk nodig hebben. Daarnaast bewaren wij de gegevens niet langer dan noodzakelijk is. Wij hanteren hiervoor verschillende bewaartermijnen die wettelijk geregeld en vastgesteld zijn. Zie bijlage.

Welke rechten hebben een leerling en ouders van leerlingen jonger dan 16 jaar

Als ouders heeft u een aantal rechten als het gaat om persoonsgegevens. Deze rechten zijn in de wet vastgelegd. Leerlingen en/of ouders kunnen op elk moment gebruik maken van deze rechten. Dit betekent bijvoorbeeld dat u altijd een verzoek kunt indienen om inzage te krijgen in de gegevens die wij van uw kind verwerken.
Daarnaast kunt u ook een verzoek indienen om gegevens te rectificeren, te beperken of helemaal te wissen uit de systemen van Stichting Scholen met de Bijbel in de Betuwe. U heeft altijd het recht om onjuiste gegevens aan te vullen of te verbeteren. Wij zullen er vervolgens voor zorgen dat deze gegevens ook bij organisaties waarmee wij deze gegevens van uw kind delen en/of uitwisselen worden aangepast.
Als u ons verzoekt om gegevens van uw kind te beperken of te wissen, zullen wij toetsen of dit mogelijk is. In deze toets houden wij ons aan de wettelijke voorschriften en kijken wij bijvoorbeeld of wij geen wettelijke plicht hebben om de gegevens te bewaren.
Tevens heeft u het recht om te vragen om de gegevens, die wij van uw kind verwerken en wij van u hebben ontvangen, aan u over te dragen of op uw verzoek aan een andere organisatie over te dragen.
Stichting Scholen met de Bijbel in de Betuwe zal geen besluiten nemen over uw kind, die alleen gebaseerd zijn op geautomatiseerde verwerking van gegevens (profiling). Beslissingen worden nooit zonder menselijke tussenkomst genomen.

Als u het niet eens bent met hoe wij omgaan met de gegevens van uw kind, dan kunt u altijd opheldering vragen bij onze Functionaris voor Gegevensbescherming (zie de contactgegevens bovenaan deze toelichting). Indien uw probleem volgens u niet goed wordt opgelost, dan kunt u dat melden bij Autoriteit voor de Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Opsomming van de categorieën van persoonsgegevens:

Categorie	Toelichting
• Contactgegevens	1a: naam, voornaam, e-mail, opleiding (bv. sector techniek); 1b: geboortedatum, geslacht; 1c: overige gegevens te weten: adres, postcode, woonplaats, telefoonnummer en eventueel andere voor communicatie benodigde gegevens, alsmede ook een bankrekeningnummer voor het afhandelen van betalingen;
• Leerling nummer een administratie-nummer dat geen andere informatie bevat dan bedoeld onder categorie 1	
• Nationaliteit en geboorteplaats	
• Ouders, voogd	contact gegevens van de ouders/verzorgers van leerlingen (naam, voornaam, adres, postcode, woonplaats, telefoonnummer en eventueel e-mailadres)
• Medische gegevens	gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling, voor zover deze van belang zijn bij het nemen van aanvullende maatregelen om goed onderwijs te kunnen volgen (bv. extra tijd bij toetsen);
• Godsdienst	gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het te volgen onderwijs (bijvoorbeeld: leerling vrij op bepaalde dag).
• Studievoortgang	gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten te weten: Begeleiding leerling (inclusief ontwikkelperspectief OPP) Aanwezigheidsregistratie Medisch dossier (papier) Klas, leerjaar, opleiding
• Onderwijsorganisatie	gegevens met het oog op het organiseren van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen; hieronder vallen ook lesroosters, enz.

Categorie	Toelichting
• Financiën	gegevens voor het berekenen, vastleggen en innen van inschrijvingsgelden, school- en/of lesgelden, bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten. (denk hierbij aan een bankrekeningnummer van de ouders)
• Beeldmateriaal	foto's en videobeelden (met of zonder geluid) van activiteiten van de school op basis van toestemming. **Let op**: Voor pasfoto voor identificatie-doeleinden is geen toestemming nodig
• Leerkrachten /intern begeleider/ extern begeleider	gegevens van leerkrachten en begeleiders, voor zover deze gegevens van belang zijn voor de organisatie van de instelling en het geven van onderwijs, opleidingen en trainingen
• BSN (PGN)	In het onderwijs heet het BSN het persoonsgebonden nummer (PGN). Ook wel onderwijsnummer genoemd. Het PGN is hetzelfde nummer als het BSN. Scholen zijn verplicht het PGN te gebruiken in hun administratie.
• Keten-ID (Eck-Id)	Unieke iD voor de 'educatieve contentketen'. Hiermee kunnen scholen gegevens delen, zonder dat ze direct herleidbaar zijn naar leerlingen of docenten

Gedragscode ICT en internet

Bron:
Kennisnet

Bewerkt door:
Stichting Scholen met de Bijbel in de Betuwe

Versiebeheer:

Versie	Status	Datum	Naam	Omschrijving
1.0		April 2019	Marion ter Horst CED	

Bijgewerkt :

Datum	Naam	Functie	Aanpassing

Inleiding

Het gebruik van internet, computernetwerk, en e-mail is voor alle medewerkers van de school noodzakelijk om de werkzaamheden te kunnen verrichten. Bij deze werkzaamheden wordt gebruik gemaakt van veel gegevens, waaronder persoonsgegevens. De (ict)faciliteiten en de verschillende gegevens worden in dit document bedrijfsmiddelen genoemd.
Onder bedrijfsmiddelen worden in ieder geval verstaan:

- Hardware: *pc, laptop, tablet, telefoon, hardware token (tag).*
- Software (of -systemen): *alle applicaties voor het uitvoeren van de werkzaamheden, zoals de school e-mailomgeving, Microsoft Office, administratiesystemen en (online)digitaal lesmateriaal maar ook apps op (mobiele) devices.*

Informatie en (persoons)gegevens: *rapportages, leerling dossiers, gegevens in e-mails. Hierbij vraagt de verwerking van persoonsgegevens vanuit de privacywetgeving extra maatregelen.*
Internetgebruik: *het bezoeken van het World Wide Web, het gebruik van e-mail en diensten als FTP en maar ook sociale media zoals Facebook, LinkedIn, Instagram en Twitter.*

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers van Stichting Scholen met de Bijbel in de Betuwe wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor de school uit te voeren.

De afspraken in dit document gelden voor alle locaties van waaruit (school)werkzaamheden worden verricht en voor alle devices waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij Stichting Scholen met de Bijbel in de Betuwe, ook voor uitzendkrachten en tijdelijke werknemers.

Uitgangspunten gedragscode

Deze gedragscode legt regels vast voor het gebruik van de bedrijfsmiddelen door medewerkers en over de controle op de naleving hiervan.
Het doel van deze gedragscode is om de normen en uitgangspunten vast te leggen ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik
- het tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten
- de bescherming van privacy gevoelige informatie waaronder persoonsgegevens van het schoolbestuur, haar medewerkers, leerlingen en hun ouders en daarmee het beschermen van de privacy en veiligheid van alle betrokkenen
- de bescherming van vertrouwelijke informatie van het schoolbestuur, haar medewerkers, leerlingen en hun ouders
- het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen
- de bescherming van de intellectuele eigendomsrechten van het schoolbestuur en derden
- het voorkomen van negatieve publiciteit
- kosten- en capaciteitsbeheersing

De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. Stichting Scholen met de Bijbel in de Betuwe zal dan ook de controle en handhaving van deze regels conform de privacywetgeving en het algemene arbeidsrechtelijk kader uitvoeren. Hierbij is het uitgangspunt een goede balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers op de werkplek. Gegevens worden alleen verzameld en gebruikt voor deze doelen. In het bijzonder zal het bestuur de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang. Het bestuur zal mensen met toegang daartoe contractueel verplichten tot afdoende geheimhouding.

Eigen verantwoordelijkheid en privégebruik

Het gebruik van door Stichting Scholen met de Bijbel in de Betuwe verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle devices die voor schoolwerk worden gebruikt (inclusief eigen devices 'Own Device') worden niet uitgeleend of aan anderen ter beschikking gesteld zonder aanvullende (beveiligings)maatregelen. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen.

Verschillende soorten gegevens

Stichting Scholen met de Bijbel in de Betuwe is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens.
Stichting Scholen met de Bijbel in de Betuwe onderscheidt drie typen gegevens:
Openbare gegevens; dit zijn gegevens die juist voor publicatie bedoeld zijn.
Interne gegevens; dit zijn gegevens die alleen voor gebruik en verwerking binnen Stichting Scholen met de Bijbel in de Betuwe bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
Vertrouwelijke gegevens; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen Stichting Scholen met de Bijbel in de Betuwe toegankelijk zijn. Denk hierbij aan (bijzondere) persoonsgegevens, personeelsgegevens of aanbestedingsgegevens.

Persoonsgegevens verdienen bijzondere aandacht. Dit zijn gegevens die een persoon betreffen én waardoor een persoon geïdentificeerd of identificeerbaar is. Denk hierbij aan naamgegevens, emailadressen maar ook telefoonnummers van zowel collega's als leerlingen en ouders van leerlingen.

De privacywetgeving verplicht elk individu om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat Stichting Scholen met de Bijbel in de Betuwe schriftelijk afspraken maakt met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk).
Stichting Scholen met de Bijbel in de Betuwe heeft een Functionaris voor gegevensbescherming aangesteld. Deze communiceert intern de gedragsregels die horen bij het verwerken van persoonsgegevens. Persoonsgegevens moeten altijd met uiterste zorgvuldigheid verwerkt en gedeeld worden.

Als persoonsgegevens toegankelijk en of inzichtelijk zijn voor personen, die geen toegang behoren hebben tot deze gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en Stichting Scholen met de Bijbel in de Betuwe.
Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt Stichting Scholen met de Bijbel in de Betuwe afspraken over:
de verwerking en verspreiding van vertrouwelijke- en persoonsgegevens. Er worden niet meer gegevens verwerkt dan noodzakelijk om het doel te bereiken
de uitwisseling van gegevens, waarbij aan de ontvanger wordt aangegeven wat de ontvanger wel of niet mag doen met de gegevens

opslag en verspreiding van gegevens, waarbij alléén gebruik gemaakt wordt van door Stichting Scholen met de Bijbel in de Betuwe goedgekeurde bedrijfsmiddelen.

Van medewerkers van Stichting Scholen met de Bijbel in de Betuwe en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bv. personeelsdossiers, vertrouwelijke enquêtegegevens, zorgdossiers et cetera wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. Dat zij de privacywetgeving hanteren en op geen enkele wijze informatie, waarvan redelijkerwijze kan worden aangenomen dat deze vertrouwelijk of privacygevoelig is, zonder toestemming van betrokkene of leidinggevende te gebruiken en/of naar buiten te brengen.

Gedragscode

In deze gedragscode voor verantwoord gebruik van bedrijfsmiddelen geeft Stichting Scholen met de Bijbel in de Betuwe aan wat de afspraken zijn met betrekking tot verschillende onderwerpen rondom het gebruik van bedrijfsmiddelen en wat dit voor de medewerkers in de dagelijkse praktijk betekent.

Algemene normen

Iedere medewerker voldoet aan de volgende algemene normen voor 'zorgvuldigheid' (niet uitputtend):
Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht.
Voorkom het lekken van interne en vertrouwelijke informatie.
Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen. (beveiligingsmaatregelen).
Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild (bijvoorbeeld door jailbreaks).
Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering door het sturen van een e-mail aan privacy@ssbb.nl en de direct leidinggevende of een telefonische melding bij de daarvoor aangewezen persoon (Zie hiervoor de procedure meldplicht datalekken van Stichting Scholen met de Bijbel in de Betuwe).

Computergebruik

Voor het uitoefenen van de werkzaamheden stelt Stichting Scholen met de Bijbel in de Betuwe aan de medewerker computer- en netwerkfaciliteiten (ict-bedrijfsmiddelen) ter beschikking. Het gebruik van deze ict-bedrijfsmiddelen is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:
Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.
Weet welke gegevens er mogen worden gebruikt (mag iedereen het zien?) en welke ict-voorzieningen kunnen worden ingezet (is het veilig genoeg?) bij het verrichten van de verschillende schoolwerkzaamheden.

- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op. (Opslaan van gegevens in public Cloud omgevingen, zoals een persoonlijke dropbox of persoonlijke OneDrive, is niet toegestaan).
- Versleutel alle gegevens met betrekking tot Stichting Scholen met de Bijbel in de Betuwe, indien deze gegevens, om welke reden dan ook, elders opgeslagen worden.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Sluit na gebruik de computer af of log uit.
- Meld storingen van beheerde werkplekken (computer of laptop) bij ICT-er en/of locatiedirecteur

Werkplek

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen waartoe zij geen rechten hebben en/of laat gegevens niet (onbedoeld) lekken. Als aanvullende regels op computergebruik gelden voor de werkplek de volgende clean desk en clear screen regels:

- Vergrendel bij het tijdelijk verlaten van de werkplek de pc (windowstoets+L).
- Verwijder interne en vertrouwelijke documenten van het bureau bij het voor langere tijd verlaten van de werkplek (denk hieraan bij het bijwonen van een vergadering).
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via een beamer) mee kan kijken. Sluit het e-mail programma af en zorg voor een opgeruimd digitaal bureaublad.
- Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan.
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar.
- Berg de klassenmap altijd goed op bij het verlaten van het lokaal.

LET OP: Als persoonsgegevens toegankelijk/inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot die gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Weet dat beveiligingsincidenten en mogelijke datalekken gemeld moeten worden volgens de procedure meldplicht datalekken van Stichting Scholen met de Bijbel in de Betuwe. Datalekken worden gemeld via privacy@ssbb.nl en de direct leidinggevende.

Gebruik eigen devices (BYOD)

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor Stichting Scholen met de Bijbel in de Betuwe worden uitgevoerd. Het Stichting Scholen met de Bijbel in de Betuwe is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school.

Voor 'Own Devices' ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:
Beveilig het device met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode die langer is dan 4 tekens.
Vergrendel het device bij het verlaten van de werkplek (windowstoets+L).
Sla persoonsgegevens van Stichting Scholen met de Bijbel in de Betuwe niet op het eigen device op; dit is niet toegestaan.
Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot Stichting Scholen met de Bijbel in de Betuwe als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden (denk hierbij aan het eigen device).
Scheid (versleutelde)gegevens, anders dan persoonsgegevens, van Stichting Scholen met de Bijbel in de Betuwe en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen device.
Houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks).
Neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het periodiek (minimaal maandelijks) scannen van het device.

Stichting Scholen met de Bijbel in de Betuwe mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van Stichting Scholen met de Bijbel in de Betuwe moet de medewerker zelf aantonen dat de bovenstaande maatregelen worden toegepast.

Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal is niet meer weg te denken bij Stichting Scholen met de Bijbel in de Betuwe. Dit lesmateriaal staat steeds meer online waarbij steeds vaker persoonsgegevens worden uitgewisseld. De privacywetgeving eist dat elke organisatie vooraf aan het gebruik van dergelijk materiaal bekijkt wat de invloed ervan is op de privacy, dit kan specifieke maatregelen tot gevolg hebben.
De onderstaande regels gelden voor installatie en gebruik van software en (online)digitaal lesmateriaal:

- Installeren van software wordt bij Stichting Scholen met de Bijbel in de Betuwe alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen.
- Bij het gebruik van online software, app's en digitaal lesmateriaal, wordt gekeken of er persoonsgegevens bij verwerkt worden.
- Een verwerkersovereenkomst wordt op bestuursniveau afgesloten met elke leverancier van (online)software, die in opdracht van Stichting Scholen met de Bijbel in de Betuwe persoonsgegevens verwerkt. Regel dit vooraf aan het gebruik.
- Aanvragen van digitaal lesmateriaal en/of andere software volgt bij Stichting Scholen met de Bijbel in de Betuwe de afgesproken aanvraagprocedure. Hiervoor is een aanvraagformulier beschikbaar wat als uitgangspunt dient voor eventuele wettelijk verplichte aanvullende privacy- en/of beveiligingsmaatregelen.

Gebruik van e-mail

Stichting Scholen met de Bijbel in de Betuwe stelt een e-mailsysteem en een bijbehorende mailbox aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik van e-mailfaciliteiten is verbonden aan deze werkzaamheden en gaan uit van de volgende afspraken:

- Gebruik het school e-mail adres alléén voor school gerelateerde zaken.
- Gebruik voor privé e-mail een eigen privé e-mailadres via een externe webmaildienst. (bijvoorbeeld webmail van Gmail, Hotmail of een eigen provider).
- Ontvangen van privémail op het school e-mailadres is incidenteel toegestaan.
- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.
- Het is niet toegestaan e-mail te gebruiken voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of voor berichten die kunnen aanzetten tot haat en geweld.
- Synchroniseert een medewerker de school e-mail met een eigen devices (tablet, telefoon) dan dient de medewerker bij verlies of diefstal van het device, gebruik te maken van de mogelijkheid om de e-mail op afstand te wissen of de device in de fabrieksinstellingen te zetten, ook als daarmee alle (privé)gegevens van het device gewist worden.
- Bij langdurige afwezigheid kan de bestuurder besluiten de mailbox te laten openen om lopende zaken voortgang te geven.
- Bij het vermoeden van misbruik van een van bovenstaande punten, kan de bestuurder ook besluiten de mailbox te openen. Hier ligt een gemotiveerd besluit onder.

Gebruik van internet

Stichting Scholen met de Bijbel in de Betuwe stelt het gebruik van internet en de bijbehorende faciliteiten aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik hiervan is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Beperkt persoonlijk gebruik is toegestaan, mits dit
  - niet storend is voor de dagelijkse werkzaamheden
  - niet voor commerciële doeleinden is en
  - geen verboden gebruik oplevert.
- Het is niet toegestaan om
  - op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten
  - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron
  - onder lestijd internettoegang te gebruiken voor privédoeleinden
  - deel te nemen aan kansspelen.

Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale netwerken en andere vergelijkbare communicatienetwerken over alle aan school verbonden betrokkenen en activiteiten. Dit geldt in het bijzonder ook voor internetgebruik buiten het schoolnetwerk met betrekking tot aan de school verbonden betrokkenen en activiteiten.

Veilig online

We brengen met z'n allen steeds meer tijd online door. Hierbij worden steeds meer mobiele devices gebruikt. Menselijk (online)handelen staat veelal aan de basis van een datalek.

Stichting Scholen met de Bijbel in de Betuwe verwacht van medewerkers dat zij:

het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken) en websites

bij het verwerken van persoonsgegevens alléén gebruik maken van bekende én beveiligde draadloze netwerken
weten wat malware is, het kunnen herkennen en weten hoe te handelen
terughoudend zijn met het online achterlaten van gegevens met betrekking tot Stichting Scholen met de Bijbel in de Betuwe

Sociale media

Sociale media is een verzamelnaam voor alle internettoepassingen die het mogelijk maken om informatie met elkaar te delen op een eenvoudige en vaak leuke manier. Het gaat hierbij niet alleen om informatie in de vorm van tekst (nieuws, artikelen). Ook geluid (podcasts, muziek) en beeld (fotografie, video) worden gedeeld via social media (Instagram, YouTube, Facebook, Twitter enz). De essentie van sociale media is dat iemand er informatie deelt over zichzelf, over anderen of over een bepaald onderwerp.
Voor gebruik van sociale media geldt als uitgangspunt dat het digitale gedrag op sociale media niet afwijkt van het real life gedrag binnen de school. Medewerkers zijn altijd de vertegenwoordiger van Stichting Scholen met de Bijbel in de Betuwe ook als zij online een privémening verkondigen. Van belang is te beseffen dat je met berichten op sociale media (onbewust) de goede naam van de school en betrokkenen ook kunt schaden. Om deze reden vragen wij om bewust om te gaan met de sociale media.
Bij Stichting Scholen met de Bijbel in de Betuwe gelden de volgende afspraken voor het gebruik van sociale media:
Deel op verantwoorde wijze kennis via sociale media rekening houdend met de goede naam van Stichting Scholen met de Bijbel in de Betuwe en iedereen die hierbij betrokken is.
Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens Stichting Scholen met de Bijbel in de Betuwe gedaan wordt.
Publiceer geen vertrouwelijke informatie en/of persoonsgegevens op sociale media.
Publiceer geen beeldmateriaal van leerlingen en medewerkers zonder de uitdrukkelijke voorafgaande aantoonbare toestemming van ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder is dan 16 jaar.
Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn. Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren.
Neem contact op met een leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met Stichting Scholen met de Bijbel in de Betuwe.
Het is medewerkers toegestaan om met een privé account ‘vrienden’ te worden met ouders op sociale media, mits ze geen privacygevoelige informatie van leerlingen, collega’s en ouders uitwisselen en geen negatieve informatie verstrekken middels een digitaal platform dat niet door de school beheerd wordt. Medewerkers mogen geen vrienden worden met leerlingen onder de 16 zonder expliciete toestemming van de ouders.
Inzetten van sociale media in het lesprogramma is gebonden aan de toestemming van ouders als leerlingen jonger zijn dan 16 jaar.

Gebruik beeld- en geluidsmateriaal

Het gebruiken van beeld- en geluidsmateriaal, het delen van foto's, video's en geluidsfragmenten van leerlingen door medewerkers vallend onder Stichting Scholen met de Bijbel in de Betuwe mag alleen als daar vooraf toestemming voor gegeven is door ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder dan 16 jaar is. Zonder deze toestemming mogen geen foto's, video's en geluidsfragmenten van leerlingen gebruikt worden.

- Stichting Scholen met de Bijbel in de Betuwe verwijst hierbij naar de richtlijn die is opgesteld voor het gebruik en toestemming van beeldmateriaal.
- Voor de afspraken rondom het delen van beeld- en geluidsmateriaal via sociale media gelden de richtlijnen die genoemd worden bij het gebruik van sociale media.

Wachtwoorden en pincodes

Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en devices (pc, laptop, telefoon) begint met een goed wachtwoord. Een lang wachtwoord of een 'wachtzin' is beter dan een kort, complex wachtwoord. Voor het gebruik van wachtwoorden gelden onderstaande afspraken:

- Wachtwoorden moeten minimaal 9 tekens bevatten, met minstens drie van de volgende vier elementen : kleine letter, hoofdletter, cijfer of speciaal teken (!@#$%^&*()
- Pincodes (op telefoon of tablet) moeten langer zijn dan 4 tekens.
- Wachtwoorden moeten volgens de afspraken binnen Stichting Scholen met de Bijbel in de Betuwe op aangegeven tijden vervangen worden.
- Gebruik niet voor elke systeem hetzelfde wachtwoord.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.

Meldplicht Datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens de procedure meldplicht datalekken van Stichting Scholen met de Bijbel in de Betuwe.
Datalekken worden gemeld via privacy@ssbb.nl en bij de direct leidinggevende.

Controle gebruik bedrijfsmiddelen

Stichting Scholen met de Bijbel in de Betuwe handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:
De Grondwet,
Algemene Verordening Gegevensbescherming
Wet Medezeggenschap Onderwijs (WMO)
Burgerlijk Wetboek (BW)
Wetboek van Strafrecht
Cao PO en
Cao VO.

Het Stichting Scholen met de Bijbel in de Betuwe zal bij controle rondom het gebruik van bedrijfsmiddelen op basis van deze gedragscode uitgaan van de juiste balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers.

Voorwaarden voor controle

Controle van persoonsgegevens met betrekking tot gebruik van bedrijfsmiddelen vindt slechts plaats in het kader van handhaving van de doelen van deze gedragscode.
Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode, in opdracht van Stichting Scholen met de Bijbel in de Betuwe gerichte controle plaatsvinden.
Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van Stichting Scholen met de Bijbel in de Betuwe, controle op de inhoud plaats.
Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.

Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken medewerker besproken. Stichting Scholen met de Bijbel in de Betuwe zal de medewerker op verzoek inzage verschaffen in de gegevens over het eigen gebruik. De medewerker wordt gewezen op de consequenties wanneer niet wordt gestopt met het ongeoorloofd gebruik.
E-mailberichten van leden van de (G)MR onderling, van vertrouwenspersonen, bedrijfsartsen en van een ieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Dit geldt niet voor veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.

Uitvoering van de controle

De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering.
De controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.
De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens. controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.
De afdeling ict, de systeembeheerder(s) zijn aan geheimhouding gebonden als men om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.
Door Stichting Scholen met de Bijbel in de Betuwe worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
Door Stichting Scholen met de Bijbel in de Betuwe worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

Disciplinaire maatregelen

Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het bestuur van Stichting Scholen met de Bijbel in de Betuwe, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen. Hieronder vallen o.a. een waarschuwing/berisping, schadevergoeding, aangifte bij de politie, overplaatsing, schorsing en/of beëindiging van de arbeidsovereenkomst.
Medewerkers die zich niet aan deze gedragscode houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken. Zij krijgen daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. Medewerker en leidinggevende maken dan afspraken voor de toekomst en bepalen de mogelijke maatregelen bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in deze gedragscode bepaalde. Ook kan de toegang tot e-mail of internet worden beperkt of geheel worden afgesloten. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens worden getroffen, zoals een constatering van een automatisch filter of blokkade. Er worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

Bezwaar en beroep

Als de medewerker het niet eens is met de (voorgenomen) disciplinaire maatregel, dan kan daar in een aantal gevallen bezwaar en/of beroep tegen worden ingesteld. Dit is meestal geregeld in de arbeidsovereenkomst, regels rondom personeelszaken en/of de van toepassing zijnde CAO.

(G)MR

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle

van het gedrag of de prestaties van medewerkers. Het medezeggenschapsorgaan (de (G)MR) is om deze reden instemmingsplichtig. Dit orgaan heeft in ? ingestemd met de inhoud van deze gedragscode.

De organisatie kan deze gedragscode met instemming van de (G)MR wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering ervan aan de medewerkers bekend gemaakt.

Slotbepaling

Deze regeling wordt elke twee jaar geëvalueerd door Stichting Scholen met de Bijbel in de Betuwe en de (G)MR. De eerstkomende evaluatie vindt plaats gelijktijdig met de evaluatie IBP.

Reglement cameratoezicht

Reglement cameratoezicht Stichting Scholen met de Bijbel in de Betuwe

Dit reglement cameratoezicht heeft betrekking op alle locaties van de Stichting Scholen met de Bijbel in de Betuwe waar toezicht door middel van camerasystemen wordt ingezet. Het geeft een beschrijving van taken, verantwoordelijkheden en procedures over het cameratoezicht, met het oog op integer gebruik van het camerasysteem en de bescherming van privacy van leerlingen, medewerkers en bezoekers.

Artikel 1 – Begripsbepalingen

1. In dit reglement wordt verstaan onder:
   a. Cameratoezicht: toezicht met behulp van camera's, waardoor er sprake is van verwerking van persoonsgegevens als bedoeld in de Algemene Verordening Gegevensbescherming.
   b. Heimelijk cameratoezicht: toezicht met behulp van verborgen en/of niet-zichtbare camera's, of cameratoezicht dat niet kenbaar is gemaakt aan leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers.
   c. Serverruimte: de van een toegangscontrolesysteem voorziene ruimte, waar de server of opnameapparatuur staat waarop de opgenomen camerabeelden geregistreerd staan.
   d. Camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, verbindingskasten, verbindingen en bevestigen waarmee het cameratoezicht wordt uitgevoerd.
   e. Camera observatieruimte: een centraal gesitueerde, van een toegangscontrolesysteem voorziene ruimte, waarin de camerabeelden - van alle locaties - centraal live worden bekeken en/of waar ook de mogelijkheid bestaat om opgenomen camerabeelden terug te kijken en/of op een informatiedrager te plaatsen.
   f. Camerabeeld: de door het cameratoezicht verkregen camerabeeld.
   g. Beheerder: de door het college van bestuur/bestuur aangewezen medewerker van de onderwijsinstelling, die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht.
   h. Locatiebeheerder: een door het college van bestuur/bestuur als zodanig aangewezen persoon die belast is met het cameratoezicht op één of meerdere locaties van de onderwijsinstelling.
   i. Technisch beheerder: de functionaris, die onder verantwoordelijkheid van de beheerder, is belast met het technisch beheer van het camerasysteem.
   j. Incident: een waargenomen ongewenst en/of strafbaar feit, ongeval of andere gebeurtenis die vraagt om handhaving, onderzoek en/of strafrechtelijke vervolging.

Artikel 2 –Werkingssfeer en doelstellingen cameratoezicht

1. Dit reglement is van toepassing op leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers die zich bevinden in de gebouwen of op de terreinen van de Stichting Scholen met de Bijbel in de Betuwe.
2. Het inzetten van cameratoezicht, en het gebruik van de camerabeelden, is alleen toegestaan voor:
   a. de bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers;
   b. de beveiliging van de toegang tot gebouwen en terreinen, waaronder mede is begrepen het weren van ongewenste bezoekers;
   c. de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
   d. het vastleggen van incidenten.
3. Camerabeelden worden uitsluitend gebruikt ten behoeve van de doelstelling zoals genoemd in lid 1.

Artikel 3 – Taken en verantwoordelijkheden

1. Het cameratoezicht geschiedt onder verantwoordelijkheid van de Stichting Scholen met de Bijbel in de Betuwe.
2. Alvorens te besluiten tot het instellen of intensiveren van cameratoezicht, voert de Stichting Scholen met de Bijbel in de Betuwe een privacytoets uit, waarbij de mate van inbreuk op de privacy van de leerlingen, medewerkers en bezoekers wordt afgewogen tegen het belang van de onderwijsinstelling om cameratoezicht te gebruiken. Hierbij wordt meegewogen of de doelstellingen als geformuleerd in artikel 2, op een andere wijze kunnen worden bereikt, met een minder ingrijpend middel dan cameratoezicht.
3. Stichting Scholen met de Bijbel in de Betuwe wijst een beheerder aan die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht binnen de onderwijsinstelling, alsmede een technisch beheerder die, onder verantwoordelijkheid van de beheerder, belast is met het technisch beheer van het camerasysteem.
4. De beheerder wijst bevoegde medewerkers aan, en zo nodig een of meer locatiebeheerder(s).
5. De beheerder wijst voor zichzelf en voor de locatiebeheerder een plaatsvervanger aan, die in geval van afwezigheid van de beheerder respectievelijk locatiebeheerder in diens taken en verantwoordelijkheden treedt.
6. De beheerder, locatiebeheerder(directeur) en bevoegde medewerkers zijn bevoegd tot het live uitkijken van camerabeelden.
7. De beheerder en locatiebeheerder (directeur) zijn bevoegd tot het terugkijken en uitgeven van opgenomen camerabeelden.
8. De beheerder en locatiebeheerder(directeur) kunnen een bevoegde medewerker autoriseren om – onder verantwoordelijkheid van de beheerder of locatiebeheerder - onder nader te stellen voorwaarden en voor een vooraf bepaald doel cq. een vooraf bepaalde periode camerabeelden terug te kijken.

Artikel 4 – Inrichten camerasysteem en beveiliging

1. De beheerder is verantwoordelijk voor de inrichting van het camerasysteem en de plaatsing van de camera's, binnen de kaders van de door Stichting Scholen met de Bijbel in de Betuwe uitgevoerde privacytoets als bedoeld in artikel 3 lid 2.
2. De beheerder zorgt voor passende technische en organisatorische maatregelen om de camerabeelden te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. Deze maatregelen garanderen, rekening houdend met de stand van de techniek (zoals te doen gebruikelijk in de informatiebeveiligings- en beveiligingsbranche) en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's van het cameratoezicht en de aard van te beschermen camerabeelden met zich meebrengen. De maatregelen betreffen het camerasysteem, de serverruimte en camera observatieruimte.
3. Het terugkijken van opgenomen camerabeelden geschiedt slechts in aanwezigheid van twee daartoe bevoegd verklaarde personen.
4. De met cameratoezicht belaste medewerkers gaan vertrouwelijk en integer om met de kennis die zij tot zich krijgen vanwege het cameratoezicht, in het bijzonder met betrekking tot de privacy van leerlingen, medewerkers en bezoekers. Voor zover daar arbeidsrechtelijk niet in is voorzien, sluit de beheerder daartoe een geheimhoudingsverklaring met de locatiebeheerder(s), technisch beheerder en/of bevoegde medewerker(s).
5. De beheerder draagt er zorg voor dat het cameratoezicht kenbaar wordt gemaakt aan leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers op zichtbare en herkenbare wijze, zoals maar niet beperkt tot borden en stickers bij de ingang van de gebouwen of terreinen van de onderwijsinstelling.
6. Voor zover er in het camerasysteem camerabeelden worden opgeslagen, worden deze beelden **na uiterlijk vier weken na de opname automatisch gewist**, tenzij er een incident is geconstateerd op basis waarvan het noodzakelijk is de met het incident samenhangende camerabeelden te bewaren. Na afhandeling van het incident worden de betreffende camerabeelden (en eventueel gemaakte kopieën of afdrukken) gewist.

7. Het camerasysteem is zodanig uitgerust dat het terugkijken van opgenomen camerabeelden of het uitgeven daarvan slechts mogelijk is in de camera observatieruimte of via een app waar alleen de locatiebeheerder toegang toe heeft.
8. Voor zover er live camerabeelden worden uitgekeken in een andere ruimte dan de serverruimte of camera observatieruimte, zijn er technische en organisatorische maatregelen genomen die het onbevoegd meekijken zoveel als redelijkerwijs mogelijk voorkomen.
9. Voor zover er bij het inrichten van het camerasysteem voor gekozen wordt om de leerlingen, medewerkers en bezoekers via een monitor live terugkoppeling te geven van de camerabeelden, kunnen deze live camerabeelden alleen betrekking hebben op deze betreffende leerlingen, medewerkers en bezoekers.
10. Bewerking van camerabeelden vindt slechts plaats in het kader van het verscherpen van deze camerabeelden.

Artikel 5 – Inzage en uitgifte opgenomen camerabeelden aan derden

1. Op verzoek van politie, rechter-commissaris of (hulp)officier van justitie kan inzage worden gegeven in (opgenomen) camerabeelden in het kader van de uitoefening van diens publiekrechtelijke taak.
2. Uitgifte van camerabeelden vindt slechts plaats op *vordering* van de politie, rechter-commissaris of (hulp)officier van justitie waarbij de vordering gebaseerd is op een wettelijke grondslag.
3. Alvorens tot inzage of uitgifte over te gaan, legitimeert de betreffende functionaris zich vooraf ten overstaan van de beheerder of locatiebeheerder, en tekent voor ontvangst van de uitgegeven camerabeelden.
4. De inzage en uitgifte wordt door de beheerder of locatiebeheerder geregistreerd.
5. Aan andere derden wordt geen inzage in de camerabeelden gegeven, of camerabeelden uitgegeven, anders dan met de uitdrukkelijke toestemming van de betrokken leerling en/of hun wettelijk vertegenwoordiger, medewerker of bezoeker.

Artikel 6 – Rechten van betrokkenen

1. Betrokken leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers komen de rechten toe zoals bedoeld in de Algemene Verordening Gegevensbescherming (tot 25 mei 2018 de Wet bescherming persoonsgegevens). Hieronder vallen het recht op inzage, correctie en verwijdering van camerabeelden waarop zij zijn afgebeeld.
2. Een verzoek tot inzage in camerabeelden geschiedt schriftelijk of per e-mail aan de beheerder, die binnen 10 werkdagen na ontvangst van het verzoek inhoudelijk zal reageren.
3. Het verzoek tot inzage wordt afgewezen wanneer het verzoek tot inzage in camerabeelden ongespecificeerd is, of als met dit verzoek kennelijk misbruikt van recht wordt gemaakt.
4. In geval van een incident, kan een inzageverzoek worden geweigerd als dat noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.
5. Klachten over de toepassing van het camerasysteem, dit reglement en over het gedrag van de beheerder, locatiebeheerder of de bevoegde medewerkers, worden schriftelijk ingediend bij Stichting Scholen met de Bijbel in de Betuwe. Stichting Scholen met de Bijbel in de Betuwe zal binnen 6 weken na datum ontvangst van de klacht reageren.

Artikel 7– Heimelijk cameratoezicht

1. Heimelijk cameratoezicht is slechts toegestaan indien regulier cameratoezicht en andere door de onderwijsinstelling genomen maatregelen en inspanningen, niet leiden tot beëindiging van de structurele incidenten. Het inzetten van heimelijk cameratoezicht is niet mogelijk voor preventieve doeleinden.
2. Voornoemd heimelijk cameratoezicht mag alleen tijdelijk en op zodanige wijze worden ingezet, dat inbreuk op de persoonlijke levenssfeer van de leerlingen, medewerkers en bezoekers zo klein mogelijk is.

3. Heimelijk cameratoezicht is uitsluitend toegestaan na specifieke voorafgaande schriftelijke toestemming van Stichting Scholen met de Bijbel in de Betuwe onder vermelding van de voorwaarden waaronder het heimelijk cameratoezicht plaatsvindt.
4. De onderwijsinstelling informeert – voor zover redelijkerwijs mogelijk - achteraf de betrokken leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers over het toegepaste heimelijk cameratoezicht.
5. Voordat heimelijk cameratoezicht wordt toegepast, moet er eerst een DPIA uitgevoerd worden. Ook als het heimelijk cameratoezicht incidenteel is.

Artikel 8 – Verslaglegging en rapportage

1. De beheerder rapporteert tenminste jaarlijks aan het College van Bestuur/bestuur over het toegepaste cameratoezicht, waaronder begrepen is een verslag over de verstrekkingen van camerabeelden zoals bedoeld in artikel 5.
2. Jaarlijks wordt door het Stichting Scholen met de Bijbel in de Betuwe gerapporteerd aan de GMR over het cameratoezicht betreffende het voorafgaande jaar (over aard, frequentie en lengte van het toezicht). Daarbij wordt specifiek gemeld indien heimelijk cameratoezicht is toegepast.

Artikel 9 – Slotbepaling

1. Stichting Scholen met de Bijbel in de Betuwe stelt dit reglement vast. Voorafgaand aan het vaststellen, wijzigen of intrekken van dit reglement cameratoezicht, vraagt Stichting Scholen met de Bijbel in de Betuwe de GMR om instemming.
2. Het reglement treedt onmiddellijk in werking. Een wijziging in dit reglement treedt in werking binnen 30 dagen na bekendmaking van de wijziging.

Informatiebeveiligings- en privacy beleid (versie 2.0)

Bron
Kennisnet

Bewerkt door:
Stichting Scholen met de Bijbel in de Betuwe

Versie	Status	Datum	Auteur	Omschrijving
1.0	Definitief	April 2019	Marion ter Horst CED	

Vastgesteld door Stichting Scholen met de Bijbel in de Betuwe:

Versie	Datum	Naam	Functie
1.0	April 2019	M.J. van der Mark	Gemandateerd bestuurder

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.

Toelichting informatiebeveiliging en privacy

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 van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

Toelichting 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.

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 op informatiebeveiliging en privacy binnen Stichting Scholen met de Bijbel in de Betuwe te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

Doel en reikwijdte

Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Stichting Scholen met de Bijbel in de Betuwe 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 Stichting Scholen met de Bijbel in de Betuwe voldoet aan relevante wet- en regelgeving.

Reikwijdte

- Het IBP-beleid binnen Stichting Scholen met de Bijbel in de Betuwe 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 Stichting Scholen met de Bijbel in de Betuwe waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting Scholen met de Bijbel in de Betuwe persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting Scholen met de Bijbel in de Betuwe. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd.
- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Stichting Scholen met de Bijbel in de Betuwe 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 Stichting Scholen met de Bijbel in de Betuwe 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 – Hoe doen we dat?

Stichting Scholen met de Bijbel in de Betuwe hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Stichting Scholen met de Bijbel in de Betuwe 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. Stichting Scholen met de Bijbel in de Betuwe voldoet aan alle relevante wet- en regelgeving.

3. Bij Stichting Scholen met de Bijbel in de Betuwe 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 Stichting Scholen met de Bijbel in de Betuwe 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 te allen tijde hun toestemming herzien.

4. Stichting Scholen met de Bijbel in de Betuwe 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. Stichting Scholen met de Bijbel in de Betuwe legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Stichting Scholen met de Bijbel in de Betuwe voldoet hiermee aan de documentatieplicht.

6. Binnen Stichting Scholen met de Bijbel in de Betuwe 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. Stichting Scholen met de Bijbel in de Betuwe 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. Stichting Scholen met de Bijbel in de Betuwe 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 tenemen maatregelen.

9. Stichting Scholen met de Bijbel in de Betuwe 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. Stichting Scholen met de Bijbel in de Betuwe 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. Stichting Scholen met de Bijbel in de Betuwe heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij Stichting Scholen met de Bijbel in de Betuwe een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. Stichting Scholen met de Bijbel in de Betuwe 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. Stichting Scholen met de Bijbel in de Betuwe 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. Stichting Scholen met de Bijbel in de Betuwe zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen

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.

Relevante wet- en regelgeving

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

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

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.

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**: 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.

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.

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, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de Privacy Officer met het bestuur als eindverantwoordelijke.

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.

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@ssbb.nl .
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

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 Stichting Scholen met de Bijbel in de Betuwe 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.

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 de 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 Stichting Scholen met de Bijbel in de Betuwe de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

Logging en monitoring

Logging en monitoring door de IT-afdeling 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.

Organisatie - Wie doet wat?

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 bij Stichting Scholen met de Bijbel in de Betuwe.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Bestuur (Raad van Toezicht)	• 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
	Werkgroep IBP (Algemeen directeur, FG, privacy officier en CED medewerker)	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse	Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik

		• 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	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	• Toezicht op naleving privacy wetgeving • Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.: ICT, HRM / P&O, facilitair, onderwijs, financiën, inkoop en administratie	• Classificatie / risicoanalyse in samenwerking met de werkgroep IBP • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie • 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

Uitvoerend (operationeel)	Privacy Officer Functioneel en/of applicatie beheerder Medewerker Dagelijkse leiding / leidinggevende / directie	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • 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 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	
Procedure rondom training medewerkers	(bewustzijn creëren)
Cameratoezicht	
Wachtwoordbeleid	
Responsible disclosure	
Gedragscode ict en internetgebruik	
Acceptable use policy	(verantwoord gebruik bedrijfsmiddelen)
Procedure rondom uitwisselen gegevens	(passend onderwijs, leerling dossiers, leerplicht enz)

Verplicht vanuit de AVG:

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

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.

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

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Stichting Scholen met de Bijbel in de Betuwe 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

Eindverantwoordelijke
Het bestuur (Raad van Toezicht) 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 werkgroep IBP.

Sturend

Werkgroep IBP
De werkgroep IBP (bestaande uit Privacy officer, Functionaris voor Gegevens bescherming, algemeen directeur en medewerker CED) is een rol op sturend niveau. Zij geven terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De werkgroep IBP moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen Stichting Scholen met de Bijbel in de Betuwe
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen Stichting Scholen met de Bijbel in de Betuwe coördineren

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG), houdt binnen Stichting Scholen met de Bijbel in de Betuwe 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 bestuur). De FG heeft regelmatig overleg met de werkgroep IBP. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

De ICT-ers en de locatiedirecteuren zijn gesprekspartners voor de werkgroep IBP in kader van informatiebeveiliging en privacy binnen de organisatie.

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 denken gespecialiseerde medewerkers mee met de werkgroep IBP. De werkgroep blijft verantwoordelijk.

De werkgroep 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:

- Zij adviseren de werkgroep IBP en denken mee m.b.t. het beleid voor toegang (autorisaties).
- Zij zien er mede 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.
- Zij beoordelen periodiek de toegangsrechten van de gebruikers.

Uitvoerend

Privacy Officer
De Privacy Officer vormt het aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Functioneel beheerder of Applicatiebeheerder
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 werkgroep IBP 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 en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelshandboek en de handleiding acceptabel gebruikmaken van bedrijfsmiddelen. 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)

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 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 werkgroep IBP. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Bijlage 3: Regeling Taken en bevoegdheden Functionaris Gegevensbescherming

Versie d.d. 23 juli 2018

Inleiding
Stichting Scholen met de Bijbel in de Betuwe (hierna SSBB) heeft besloten de functie van Functionaris Gegevensbescherming (hierna: FG) uit te besteden aan Lumen Group. Gedurende de looptijd van het abonnement is bijgaande regeling met taken en bevoegdheden, die gebaseerd zijn op artikelen 37-39 uit de Algemene Verordening Gegevensbescherming (hierna: AVG), van toepassing.

De AVG vereist dat een natuurlijk persoon de functie van Functionaris Gegevensbescherming vervult. Binnen Lumen Group zal de heer S.S. Sarneel deze functie van FG op zich te nemen voor SSBB. Bij de Autoriteit Persoonsgegevens zijn de heer Sarneel en Lumen Group voor SSBB reeds aangemeld als zijnde uw FG.

Artikel 1: definities
a. AVG: Algemene Verordening Gegevensbescherming;
b. FG: functionaris voor gegevensbescherming artikel 37 van de AVG;
c. Verwerkingsverantwoordelijke: het bestuur van SSBB;
d. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, bedrijf, organisatie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt;
e. Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (betrokkene) waarbij als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
f. Verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
g. Personeel: medewerkers in loondienst en/of extern ingehuurde medewerkers die in opdracht van de Verwerkingsverantwoordelijke werkzaamheden verrichten.

Artikel 2: Taken FG
Aanvullende op de afgesproken diensten binnen het abonnement zoals vastgelegd in de ondertekende offerte, heeft de FG de volgende wettelijke taken:
a. het houden van toezicht op verwerkingen van persoonsgegevens. Dit houdt onder meer in een risico-gebaseerde monitoring op naleving van de AVG door uw organisatie. Dit richt zich onder meer op: beleid, getroffen technische- en organisatorische maatregelen, bewustmaking personeel en audits verband houdende met de bescherming van persoonsgegevens;

b. toezicht houden op wijzigingen in bestaande verwerkingen en/of het nieuwe verwerkingen met persoonsgegevens. Het personeel meldt bij de FG alle (nieuwe) verwerkingen van persoonsgegevens alsmede eventuele incidenten met betrekking tot privacy en informatiebeveiliging;
c. geven van (ongevraagd) advies en doen van aanbevelingen over privacy en informatiebeveiliging in het algemeen en de toepassing van de AVG;
d. contactpersoon richting Autoriteit Persoonsgegevens indien afstemming of samenwerking nodig is met de toezichthouder;
e. opstellen van een verslag van zijn werkzaamheden. Twee keer per jaar een onafhankelijke rapportage van de FG met eventuele bevindingen en aanbevelingen. Bespreking van de rapportage op locatie met hoogste management (inclusief jaarlijkse evaluatie van onze dienstverlening);
f. het (laten) afhandelen van klachten, opmerkingen of vragen van betrokkenen inzake privacy en informatiebeveiliging. De FG is bereikbaar voor klachten, opmerkingen en vragen van betrokkenen via e-mail /website.

Artikel 3: Bevoegdheden FG
1. De FG is bevoegd, zo nodig met medeneming van de benodigde apparatuur, elke plaats in de gebouwen op de terreinen in gebruik zijn en waar persoonsgegevens worden verwerkt, te betreden.
2. De FG is bevoegd inlichtingen te vorderen van een ieder die onder gezag of in opdracht van werkzaam is of overeenkomstig voor of namens SSBB persoonsgegevens verwerkt.
3. De FG is bevoegd inzage te vorderen van zakelijke gegevens en bescheiden waarin persoonsgegevens zijn verwerkt.
4. De FG is bevoegd van de gegevens en bescheiden kopieën te maken.
5. Indien het maken van kopieën niet ter plekke kan gebeuren, is hij bevoegd de gegevens en bescheiden voor de duur van maximaal één werkdag mee te nemen.
6. De FG is bevoegd tot het geven van een opdracht tot het aanmaken van een registratie van persoonsgegevens in overeenstemming met de AVG. Ook is de FG bevoegd tot het geven van een opdracht voor de vernietiging van persoonsgegevens, waarvan de bewaartermijn is overschreden of indien de gegevensverwerking onrechtmatig is.
7. De FG is bevoegd zich te laten vergezellen en bijstaan door personen die daartoe door hem zijn aangewezen.
8. De FG maakt van de bevoegdheden als bedoeld in deze artikelen slechts gebruik voor zover dit redelijkerwijs voor de uitoefening van de taak noodzakelijk is.

Artikel 4: Waarborgen onafhankelijke FG
SSBB zorgt er voor dat:
a. de FG onafhankelijk kan werken en geen instructies ontvangt van SSBB hoe de FG zijn taken moet uitvoeren;
b. De FG krijgt actieve steun vanuit de directie en de interne organisatie en wordt proactief en tijdig geïnformeerd over alle aangelegenheden die raakvlakken hebben met de bescherming van persoonsgegevens. Hieronder vallen ook (potentiele) datalekken en data gedreven incidenten waarbij persoonsgegevens betrokken zijn.

Artikel 5: Inwerkingtreding en publicatie
Deze regeling wordt vastgesteld en gewijzigd bij besluit van de Verwerkingsverantwoordelijke.

Deze regeling treedt in werking op 1 augustus 2018 en zal intern aan het personeel bekend worden gemaakt door publicatie op 21 september 2018.

Vastgesteld door het bestuur van SSBB op 29-08-2018.

Voor akkoord,
Datum: 29-08-2018
Plaats: Veenendaal

M.J. van der Mark Gemandateerd bestuurder SSBB	Stijn Sarneel Functionaris Gegevensbescherming

Bijlage 4: Bewaartermijnen

Sollicitatiegegevens

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn	Vastgelegd in
Sollicitatiebrief, -formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant	na beëindiging sollicitatieprocedure of einde dienstverband/benoemings-termijn		art. 5 lid 6 en art. 7 lid 5 Vrijstellingsbesluit Wbp

Arbeidsovereenkomst

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn	Vastgelegd in
Akte van aanstelling / arbeidsovereenkomst	maximaal 2 jaar	einde dienstverband		art. 7 lid 5 Vrijstellingsbesluit Wbp
Wijzigingen arbeidsovereenkomst	maximaal 2 jaar	einde dienstverband		art. 7 lid 5 Vrijstellingsbesluit Wbp
Correspondentie inzake benoemingen, promotie, demotie	maximaal 2 jaar	einde dienstverband		art. 7 lid 5 Vrijstellingsbesluit Wbp
Aanspraken in verband met de beëindiging van het dienstverband	maximaal 2 jaar	datum waarop aanspraken zijn geëindigd		art. 9 lid 5 Vrijstellingsbesluit Wbp
Afspraken inzake werk MR	maximaal 2 jaar	einde lidmaatschap		art. 7 lid 5 Vrijstellingsbesluit Wbp
Burgerlijke staat werknemer	maximaal 2 jaar	einde dienstverband		art. 7 lid 5 Vrijstellingsbesluit Wbp
Kopie getuigschrift	maximaal 2 jaar	einde dienstverband		art. 9 lid 5 Vrijstellingsbesluit Wbp
Afspraken inzake opleidingen	maximaal 2 jaar	einde dienstverband		art. 7 lid 5 Vrijstellingsbesluit Wbp
Aanvraag opleiding door werknemer	maximaal 2 jaar	einde dienstverband		art. 7 lid 5 Vrijstellingsbesluit Wbp
Afspraken omtrent loopbaan	maximaal 2 jaar	einde dienstverband		art. 7 lid 5 Vrijstellingsbesluit Wbp
Verslagen functionerings- en beoordelingsgesprekken	maximaal 2 jaar	einde dienstverband		art. 7 lid 5 Vrijstellingsbesluit Wbp

Ziekte en arbeidsongeschiktheid

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn	Vastgelegd in
Correspondentie UWV en bedrijfsarts	maximaal 2 jaar	einde dienstverband		art. 7 lid 5 Vrijstellingsbesluit Wbp
Verslaglegging inzake Wet Verbetering Poortwachter	maximaal 2 jaar	einde dienstverband		art. 7 lid 5 Vrijstellingsbesluit Wbp
Verzuimregistratie als werkgever eigenrisicodrager Ziektewet is	minimaal 5 jaar De bedrijfsarts moet de gegevens minimaal 10 jaar bewaren. In verband met eigenrisicodragerschap WGA mogen de gegevens voor de duur van het WGA-traject bewaard blijven (10 jaar).	einde dienstverband dan wel in geval het dienstverband wordt voortgezet 1 januari volgend op het jaar waarin een WIA-uitkering is toegekend.		art. 3 lid 2 Regeling werkzaamheden, administratieve voorschriften en kosten eigenrisicodragen ZW

Overige personeelszaken

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn	Vastgelegd in
Verslaglegging van correspondentie met betrekking tot problematische (financiële) privé-situatie	maximaal 2 jaar	einde dienstverband		art. 7 lid 5 Vrijstellingsbesluit Wbp
Loonbeslagen	tot opheffing	-		art. 9 lid 5 Vrijstellingsbesluit Wbp
Correspondentie met betrekking tot jubilea	tot einde dienstverband	-		art. 7 lid 5 Vrijstellingsbesluit Wbp
Correspondentie directie / PZ / direct leidinggevende	afhankelijk van ontslagsituatie bij einde dienstverband of tot maximaal 2 jaar daarna	-		art. 7 lid 5 Vrijstellingsbesluit Wbp
Identiteitspapieren van derden ingeleende vreemdelingen waarvoor een tewerkstellingsvergunning is verleend	minimaal 5 jaar	einde dienstverband		art. 15 lid 4 Wet arbeid vreemdelingen

Leerlingdossier – onderwijskundig dossier

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn	Vastgelegd in

Het onderwijskundig rapport	maximaal 2 jaar	datum van uitschrijving		art. 19 lid 7 Vrijstellingsbesluit Wbp
Gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen	maximaal 2 jaar	datum van uitschrijving		art. 19 lid 7 Vrijstellingsbesluit Wbp
Gegevens over de vorderingen en de (examen)resultaten van de leerling	minimaal 6 maanden maximaal 2 jaar	datum van uitschrijving		art. 57 Examenbesluit en art. 19 lid 7 Vrijstellingsbesluit Wbp
Verslagen van gesprekken met de ouders	maximaal 2 jaar	datum van uitschrijving		art. 19 lid 7 Vrijstellingsbesluit Wbp
Gegevens die nodig zijn om te berekenen hoeveel geld de school krijgt	minimaal 7 jaar	datum van uitschrijving		art. 103a lid 3 Wvo en/of art. 172 lid 3 Wpo
Psychologisch rapport	maximaal 2 jaar Wanneer het rapport wordt opgevraagd bij een school voor po in het kader van toelating tot een school voor vo minimaal 3 en maximaal 5 jaar	datum van uitschrijving		art. 19 lid 7 Vrijstellingsbesluit Wbp
Adresgegevens	maximaal 2 jaar	datum van uitschrijving		art. 19 lid 7 Vrijstellingsbesluit Wbp
Let op! Op advies van de PO-raad hanteren wij voor leerlinggegevens een termijn van vijf jaar				

Leerlingdossier – leerplicht/ bekostiging

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn	Vastgelegd in
Gegevens over in– en uitschrijving	minimaal 5 jaar	datum van uitschrijving		art. 6 Bekostigingsbesluit Wvo en/of art. 9 Bekostigingsbesluit Wpo
Gegevens over verzuim en afwezigheid	minimaal 5 jaar	datum van uitschrijving		art. 6 Bekostigingsbesluit Wvo en/of art. 9 Bekostigingsbesluit Wpo

Adresgegevens	maximaal 2 jaar	datum van uitschrijving		art. 20 lid 5 Vrijstellingsbesluit Wbp
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school krijgt	minimaal 7 jaar	na afloop van het schooljaar waarop de bekostiging betrekking heeft		art. 103a lid 3 Wvo en/of art. 172 lid 3 Wpo
Gegevens met betrekking tot de vergoeding van de kosten verbonden aan leerlingvervoer	maximaal 2 jaar	na afloop van het schooljaar waarop de verstrekking van de vergoeding betrekking heeft		art. 21 lid 5 Vrijstellingsbesluit Wbp
Let op! Op advies van de PO-raad hanteren wij voor leerlinggegevens een termijn van vijf jaar				

Camera en videobeelden

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn	Vastgelegd in
Camera en videobeelden	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten	moment van opname		art. 38 lid 6 Vrijstellingsbesluit Wbp
Gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de video-opnamen zijn gemaakt.	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten	moment van opname		art. 38 lid 6 Vrijstellingsbesluit Wbp

Gebruik ICT-middelen en schoolnetwerk

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn	Vastgelegd in
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk door personeel en leerlingen	maximaal 6 maanden	moment van opname		art. 32 lid 6 en art. 34 lid 5 Vrijstellingsbesluit Wbp

Gegevens van leveranciers

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn	Vastgelegd in
Persoonsgegevens van (vertegenwoordigers van) leveranciers	maximaal 2 jaar	nadat de desbetreffende transactie is afgewikkeld		art. 13 lid 5 Vrijstellingsbesluit Wbp

Gegevens van huurders

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn	Vastgelegd in
Persoonsgegevens van huurders	maximaal 2 jaar	maximaal 2 jaar nadat de huur is beëindigd		art. 14 lid 5 Vrijstellingsbesluit Wbp

Gegevensdragers - belastingheffing

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn	Vastgelegd in
Loonadministratie	minimaal 7 jaar	na afloop boekjaar		art. 52 lid 4 Algemene wet inzake rijksbelastingen
Loonbelastingverklaringen en kopie identiteitsbewijs	minimaal 5 jaar	einde dienstverband		art. 23a Uitvoeringsregeling loonbelasting