

Fliers



protestants christelijke scholenvereniging

Informatiebeveiligings- en privacy beleid (IBP)

1	INLEIDING	3
2	TOELICHTING	3
2.1	TOELICHTING INFORMATIEBEVEILIGING	3
2.2	TOELICHTING PRIVACY	3
2.3	VERVLECHTING INFORMATIEBEVEILIGING EN PRIVACY	3
3	DOEL EN REIKWIJDTE	4
3.1	DOEL	4
3.2	REIKWIJDTE	4
4	UITGANGSPUNTEN	5
4.1	ALGEMENE BELEIDSUITGANGSPUNTEN	5
4.2	UITGANGSPUNTEN PRIVACY	6
5	WET- EN REGELGEVING	6
6	ORGANISATIE EN ROLLEN	7
7	CONTROLE EN RAPPORTAGE	8
7.1	VOORLICHTING EN BEWUSTZIJN	8
7.2	CLASSIFICATIE EN RISICOANALYSE	9
7.3	INCIDENTEN EN DATALEKKEN	9
7.4	CONTROLE, NALEVING EN SANCTIES	9



1 Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ICT. Deze afhankelijkheid van ICT en gegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy (IBP) om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

2 Toelichting

2.1 Toelichting informatiebeveiliging

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

Deze aspecten zijn:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

2.2 Toelichting privacy

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

2.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen Fiers.



3 Doel en reikwijdte

3.1 Doel

Dit beleid heeft als doelen:

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

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

3.2 Reikwijdte

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



4 Uitgangspunten

4.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Fiers zijn:

- Informatiebeveiliging en privacy dient te voldoen aan alle relevante wet- en regelgeving.
- De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van Fiers om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.
- Binnen Fiers 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.
- Fiers is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert Fiers informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
- De waarde van informatie wordt bij Fiers geclassificeerd. De classificatie is het uitgangspunt voor de te nemen maatregelen. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- Fiers sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant 'Digitale leermiddelen privacy' (www.privacyconvenant.nl) en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagooverlies. Fiers heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
- Informatiebeveiliging en privacy is bij Fiers een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij Fiers vanaf de start rekening gehouden met informatiebeveiliging en privacy.



4.2 Uitgangspunten privacy

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

1. **Doelbepaling en doelbinding:** persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag:** verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie:** bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel. Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie:** de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen. Zie ook het privacyreglement.

Bij alle registraties op basis van toestemming, zal Fiers aan de betrokkene een procedure worden aangeboden.

5 Wet- en regelgeving

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

- Wet op het primair onderwijs
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy' leidend bij het maken van afspraken met leveranciers die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.



6 Organisatie en rollen

Fiers heeft informatiebeveiliging en privacy (IBP) op de volgende manier intern gestructureerd en georganiseerd:

- **Alle medewerkers**
 - Gaan zorgvuldig om met privacy, persoonsgegevens en systemen en voelen zich hiervoor verantwoordelijk.
 - Kennen de gedragsregels (zie bijlage gedragscodes) van Fiers en dragen deze uit bij het uitoefenen van hun functie.
- **ICT'er**
 - Is het 1^e aanspreekpunt binnen de school voor vragen over IBP.
 - Geeft voorlichting over IBP en stimuleert bewustwording.
 - Adviseert de schoolleiding over IBP.
 - Werkt mee aan de evaluatie van het IBP-beleid en de maatregelen.
- **Schooldirecteur**
 - Communiceert over het IBP-beleid met betrokkenen in de school en ziet er op toe dat dit beleid wordt uitgevoerd.
 - Ziet toe dat persoonsgegevens zorgvuldig en rechtmatig binnen de school worden verwerkt en geeft hierbij het goede voorbeeld.
 - Zorgt dat toestemmingen van betrokkenen voor gebruik beeld- en videomateriaal etc. aanwezig en actueel zijn.
 - Draagt zorg voor archivering c.q. opschoning van de personeelsdossiers op schoolniveau die gaan over de gesprekkencyclus volgens bewaartermijnenbeleid van Fiers.
 - Draagt zorg voor archivering c.q. opschoning van het leerlingenvolgsysteem volgens bewaartermijnenbeleid van Fiers.
 - Registreert en handelt verzoeken om inzage etc. af.
 - Informeert de algemeen directeur over incidenten/datalekken.
 - Brengt regelmatig IBP onder de aandacht in werkoverleggen, beoordelingen etc.
 - Werkt mee aan de evaluatie van het IBP-beleid en de maatregelen.
- **Bovenschoolse ICT'er**
 - Is het technisch aanspreekpunt voor beveiligingsincidenten en datalekken.
 - Werkt mee aan de evaluatie van het IBP-beleid en de maatregelen.
- **Beleidsmedewerker Personeel**
 - Draagt zorg voor archivering c.q. opschoning van de personeelsadministratie en de personeelsdossiers op bestuursniveau volgens bewaartermijnenbeleid van Fiers. Deze dossiers bevatten geen gegevens over de gesprekkencyclus (zie hierboven bij schooldirecteur).
- **Functionaris gegevensbescherming (FG)**
 - Informeert en adviseert algemeen directeur, schoolleiding, ouders en personeel over IBP.
 - Houdt toezicht dat de AVG binnen de organisatie wordt nageleefd en rapporteert daarover aan de algemeen directeur.
 - Brengt op verzoek advies uit over de DPIA (privacy risicoanalyse) die de algemeen directeur wil uitvoeren en ziet toe op de uitvoering daarvan.
 - Adviseert over de afhandeling van beveiligingsincidenten en datalekken.
 - Handelt klachten af over het gebruik van persoonsgegevens of hoe een verzoek om inzage etc. is afgewikkeld.



- **Algemeen directeur**
 - Stelt het IBP-beleid vast, communiceert hierover met betrokkenen in de organisatie en ziet er op toe dat dit beleid wordt uitgevoerd.
 - Richt de organisatie qua IBP in en wijst rollen en taken toe.
 - Kent toegangsrechten personeelsadministratiesysteem toe en beheert deze.
 - Ziet toe dat persoonsgegevens zorgvuldig en rechtmatig binnen de organisatie worden verwerkt en geeft hierbij het goede voorbeeld.
 - Brengt regelmatig IBP onder de aandacht in werkoverleggen, beoordelingen etc.
 - Evalueert regelmatig het IBP-beleid en de maatregelen.
- **Toezichthoudend bestuur**
 - Ziet toe dat de organisatie IBP-beleid ontwikkelt en uitvoert.
 - Bespreekt met de algemeen directeur jaarlijks het audit-rapport van de Functionaris Gegevensbescherming en monitort eventuele vervolgacties.
- **Gemeenschappelijke medezeggenschapsraad (GMR)**

In de Wet medezeggenschap op scholen (WMS) wordt IBP als zodanig niet genoemd. Op grond van art. 12 lid 1 sub m WMS heeft de PGMR instemmingsrecht ten aanzien van de vaststelling of wijziging van een regeling over het verwerken van en de bescherming van persoonsgegevens van het personeel. De OGMR heeft op grond van art. 13 sub i WMS eenzelfde instemmingsrecht met betrekking tot persoonsgegevens van ouders en leerlingen. Vertaald naar de praktijk betekent dit dat de GMR instemmingsrecht heeft ten aanzien van:

 1. de beleidsnotitie IBP incl. plan van aanpak
 2. privacyverklaring voor leerlingen en ouders
 3. privacyverklaring voor medewerkers, studenten en vrijwilligers
 4. gedragscode sociale media
 5. protocol foto's en video's
 6. plan van aanpak informatiebeveiliging

Fiers werkt het AVG-beleid uit in procedures, formulieren etc. Ten aanzien van deze uitwerkingen heeft de GMR informatierecht.

7 Controle en rapportage

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

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

Daarnaast kent Fiers een jaarlijkse Planning & 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 meegenomen.

7.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom



wordt bij Fiers 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 beveiligingsbewustzijn is een gezamenlijke verantwoordelijkheid van de FG met het van bestuur als eindverantwoordelijke.

7.2 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang voor de informatievoorziening.

7.3 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@fiers.nu. Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

7.4 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevend 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 brede gedragscode, met periodieke bewustwordingscampagnes, enz.

Voor de bevordering van de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG is aangesteld door het bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

Mocht de naleving ernstig tekortschieten, dan kan Fiers de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden. Bij Fiers is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

