# Informatiebeveiligings- en privacy beleid (IBP)

| | |
|---|---|
| **Naam** | Openbaar Onderwijs Groningen |
| **Van** | College van Bestuur |
| **Aan** | Alle betrokkenen |
| **Datum** | 1 mei 2023 |
| **Betreft** | Informatiebeveiligings- en privacy beleid (IBP) |
| **Document** | IBP Beleid Deffinitief |

**Vastgesteld door Openbaar Onderwijs Groningen:**

| Versie | Datum | Functie | Besluit |
|---|---|---|---|
| 1.0 | 1 mei 2023 | College van Bestuur | Vastgesteld |
| 1.0 | 12 april 2023 | GMR PO | Ingestemd |
| 1.0 | 20 april 2023 | GMR VO | Ingestemd |

# Inhoud

# 1 Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ict. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ict. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ict en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

# 2 Toelichting informatiebeveiliging en privacy

## 2.1 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.

## 2.2 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.*

## 2.3 Vervlechting informatiebeveiliging en privacy

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

# 3 Doel en reikwijdte

## 3.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

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

## 3.2 Reikwijdte

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

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

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Openbaar Onderwijs Groningen. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Openbaar Onderwijs Groningen 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 Openbaar Onderwijs Groningen raakvlakken met:
  - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten onder meer: 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

## 4 Beleid – Hoe doen we dat?

Openbaar Onderwijs Groningen hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van Openbaar Onderwijs Groningen neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het college van bestuur is hierop aan te spreken. In termen van de wet is het college van bestuur de verwerkingsverantwoordelijke.

2. Openbaar Onderwijs Groningen voldoet aan alle relevante wet- en regelgeving.

3. Bij Openbaar Onderwijs Groningen 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 Openbaar Onderwijs Groningen 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. Openbaar Onderwijs Groningen zal alle betrokkenen helder en actief informeren over de verwerkingen van 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. Openbaar Onderwijs Groningen legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Openbaar Onderwijs Groningen voldoet hiermee aan de documentatieplicht.

6. Binnen Openbaar Onderwijs Groningen 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. Openbaar Onderwijs Groningen 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. Openbaar Onderwijs Groningen classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

9. Openbaar Onderwijs Groningen 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. Openbaar Onderwijs Groningen 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 ont-

staan die leiden tot schade en/of imagoverlies. Openbaar Onderwijs Groningen heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij Openbaar Onderwijs Groningen een continu proces, waarbij periodiek wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. Openbaar Onderwijs Groningen 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. Openbaar Onderwijs Groningen 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.
    Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt Openbaar Onderwijs Groningen aanvullende afspraken vast over de technische maatregelen.

14. Openbaar Onderwijs Groningen zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

# 5 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.

## 5.1 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 (AVG)
- 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.

## 5.2 Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding:** persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen (toestemming, uitvoering van overeenkomst, wettelijke verplichting, vitaal belang van betrokkene of andere personen, algemeen belang, 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 (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.

### 5.3 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

### 5.4 Voorlichting en bewustzijn

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 Security Officer met het college van bestuur als eindverantwoordelijke.

### 5.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. 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.

### 5.6 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 van datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld via het mailadres avg@o2g2.nl**.** De meldingen die hier binnenkomen worden gedeeld met de FG**.**
Periodiek zullen de beveiligingsincidenten besproken worden (door de FG, privacy-officer, security-officer en proceseigenaar) en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

### 5.7 Planning en control

Dit IBP-beleid wordt periodiek (minimaal eens per twee jaar) getoetst en bijgesteld.

Hierbij wordt rekening gehouden met:

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

Daarnaast kent Openbaar Onderwijs Groningen 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.

### 5.8 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera. Voor toezicht op de naleving van de AVG vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een het CvB vast te stellen reglement 'taken en verantwoordelijkheden FG'.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Openbaar Onderwijs Groningen de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

### 5.9 Logging en monitoring

Logging en monitoring door de ICT-afdeling zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

# 6 Organisatie - Wie doet wat?

## 6.1 Rollen en verantwoordelijkheden

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

Dit hoofdstuk beschrijft hoe IBP op drie niveaus wordt georganiseerd.

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

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken wordt bij Openbaar Onderwijs Groningen 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 College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd. Het beheer van het IBP-beleid is gemandateerd aan de Privacy Officer.

**Sturend**

**Stuurgroep**
De Stuurgroep houdt zich op sturend niveau bezig met het opzetten en onderhouden van het managementsysteem voor Informatiebeveiliging en Privacy (IBP). De Stuurgroep bestaat uit:

- Manager ICT
- Bestuurssecretaris
- Concerncontroller

**Projectgroep IBP**
De Projectgroep houdt zich inhoudelijk bezig met het opzetten van het managementsysteem voor Informatiebeveiliging en Privacy (IBP). De Projectgroep IBP bestaat uit de volgende leden:

- Projectleider IBP (extern)
- FG (extern)
- Kwartiermakers (2x extern)
- Controller
- Security Officer
- Privacy-officer

De projectgroep is tijdelijk van aard, en zal worden opgeheven na afronding van het project. Wel zal periodiek overleg worden georganiseerd tussen de FG, de security-officer en de privacy-officer.

**Privacy Officer**
De Privacy Officer (PO) is een rol op sturend niveau. De PO geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur). De PO moet:

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

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

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

- Vaststellen van het beleid voor toegang (autorisaties). Dit binnen de algemene kaders voor toegang tot ICT-systemen.
- Samen met functioneel beheer en ICT-beheer zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

**Functionaris Gegevensbescherming**
De Functionaris Gegevensbescherming (FG) houdt binnen Openbaar Onderwijs Groningen 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 college van bestuur). De FG heeft regelmatig overleg met de privacy-officer en de security-officer. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

## Uitvoerend

**Medewerker**
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in diverse beleidsdocumenten, protocollen en reglementen. 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 de regels voor informatiebeveiliging na te leven, meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).

**Leidinggevenden**
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. De dagelijkse leiding heeft op uitvoerend niveau de taak om:

- ervoor 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.

Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

## Beveiligingsincidenten en datalekken

**Incident Response Team (IRT)**
*Het Incident Response Team bij Openbaar Onderwijs Groningen bestaat uit:*

- Security Officer (incident analist)
- Functionaris Gegevensbescherming (FG)
- Privacy-Officer
- Stuurgroep

*Wat is de taak van het Incident Response Team?*
*Het IRT pakt het incident op als het om een (mogelijk) datalek gaat. De volgende actiestappen en procedures kunnen (eventueel gelijktijdig) uitgevoerd worden door dit team:*

- Lek dichten
- Formeel vaststellen datalek
- Melding bij AP
- Informeren betrokkenen
- Oplossen datalek
- Vaststellen oorzaak
- Vaststellen aansprakelijkheid
- Indien nodig: vaststellen communicatiestrategie

Het Incident Response Team heeft de verantwoordelijkheid de oorzaak van het incident te evalueren met als doel herhaling te voorkomen. Bij een datalek moet het team bovendien evalueren of het incident mogelijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkenen. Imagoschade bij het verlies van persoonsgegevens is vaak groter dan de directe financiële schade waardoor een communicatiestrategie absoluut noodzakelijk is.

Het schema van de rollen en verantwoordelijkheden is opgenomen 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 etc) |
| 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 gegevensbeschermingseffectbeoordeling | (DPIA) |
| Risicoanalyse | |
| Functionaris Gegevensbescherming | (communicatie hierover richting medewerkers) |

## Bijlage 2: Schema Rollen en verantwoordelijkheden

| | | |
|---|---|---|
| *Richtinggevend* | **Eindverantwoordelijk** | |
| | College van Bestuur | • *Eindverantwoordelijk*<br>• *IBP-beleidsvorming, -vastlegging en communiceren ervan*<br>• *Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens*<br>• *Organisatie IBP inrichten; toewijzen van de taken en rollen*<br>• *Evalueren toepassing en werking IBP-beleid op basis van rapportages* |
| *Sturend* | **Uitwerken beleid / inhoudelijk verantwoordelijk** | |
| | Stuurgroep IBP<br>Projectgroep IBP<br>Privacy Officer | • *Voorbereiden opstellen IBP-beleid, Classificatie/risicoanalyse*<br>• *Inhoudelijk verantwoordelijk voor uitwerking van het IBP-beleid*<br>• *Adviseert verwerkingsverantwoordelijke (bestuur/CvB/directie) over IBP*<br>• *Uitwerken algemeen IBP-beleid naar specifiek beleid op een uniforme manier*<br>• *Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering van het IBP-beleid te ondersteunen*<br>• *Evalueren van het IBP-beleid en de maatregelen* |
| | Functionaris Gegevensbescherming (FG) | • *Toezicht houden op naleving privacywetgeving*<br>• *Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens*<br>• *Voorlichting privacy geven en stimuleren van bewustwording*<br>• *Afwikkeling IBP-klachten en incidenten* |
| | Proceseigenaren, afdelingshoofd | • *Risicoanalyse in samenwerking met inhoudelijk verantwoordelijke*<br>• *Toegangsbeleid zowel fysieke toegang als digitale toegang vaststellen en laten goedkeuren door de verwerkingsverantwoordelijke*<br>• *Regelmatig de (netwerk)toegangsrechten van gebruikers beoordelen, controleren en vastleggen.* |
| *Uitvoerend* | **Uitvoeren beleid / naleven beleid** | |
| | • Security-officer<br>• Privacy-officer<br>• Security officer, ict-beheerder | • *Incidentafhandeling (registreren en evalueren).*<br>• *Betrokken bij incidenten met persoonsgegeven*<br>• *Technisch aanspreekpunt voor IBP-incidenten.* |
| | • Schoolleiding, managers ondersteuningsbureau<br>• Alle medewerkers | • *Uitvoeren taken conform gegeven richtlijnen en procedures.*<br>• *Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.* |
| | **Toezicht naleving en communicatie** | |
| | Toezichthouders<br>• FG<br>• Dagelijkse leiding | • *Communicatie naar alle betrokkenen; ervoor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan.*<br>• *Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers.*<br>• *Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid.*<br>• *Implementeren IBP-maatregelen.*<br>• *periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;* |