IBP beleid
Informatiebeveiliging en Privacy

Akkoord! kleurt

AKKOORD!
primair openbaar onderwijs

Bron
Kennisnet

Bewerkt door:
Stichting Akkoord!PO
Privacy Officer

Versie	Status	Datum	Auteur	Omschrijving
1.1	Definitief	26-03-2025	Leon Peters	Privacy Officer

Vastgesteld door Stichting Akkoord:

Versie	Datum	Naam	Functie
1.1	26-03-2025	Kim Schmitz GMR	CvB Akkoord!PO

1. Het normenkader IBP

Informatiebeveiliging en privacy (IBP) spelen een cruciale rol in organisaties die werken met gevoelige gegevens. Het normenkader IBP biedt een gestructureerde set richtlijnen en eisen om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen. Dit kader helpt o.a. schoolorganisaties te voldoen aan wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG).

Het normenkader IBP is gebaseerd op internationale standaarden, zoals ISO 27001 en NEN 7510, en omvat onderwerpen zoals risicobeheer, toegangscontrole, incidentmanagement en bewustwording. Door dit normenkader toe te passen, kunnen organisaties proactief beveiligingsrisico's beheersen en een veilige digitale omgeving creëren.

Akkoord!PO zal, net zoals alle schoolbesturen in Nederland, in 2027 moeten voldoen aan een volwassenheidsniveau 3 (van 5). Dit is een forse opdracht. We beginnen bij Akkoord!PO niet bij nul; veel zaken zijn al in gang gezet en worden momenteel geactualiseerd. Zo ook dit **beleidsplan IBP**. Het beleidsplan IBP vormt de basis voor alle activiteiten die de stichting moet uitvoeren om het volwassenheidsniveau 3 te bereiken.

Kenmerken van volwassenheidsniveau 3 IBP:

1. Gestandaardiseerde processen – Informatiebeveiliging en privacymaatregelen zijn formeel gedocumenteerd en vastgesteld binnen de organisatie.
2. Consistente uitvoering – Medewerkers voeren IBP-processen volgens vastgestelde richtlijnen uit, waardoor minder afhankelijkheid van individuen ontstaat.
3. Bewustwording en training – Medewerkers zijn op de hoogte van IBP-beleid en worden regelmatig getraind om zich aan de richtlijnen te houden.
4. Monitoring en controle – Er zijn mechanismen ingeregeld om naleving van het IBP-beleid te controleren, zoals audits en rapportages.
5. Formele rollen en verantwoordelijkheden (governance) – IBP is toegewezen aan specifieke functionarissen (bijv. FG, Privacy Officer) en wordt structureel beheerd (zie bijlage 2).

Waarom is niveau 3 belangrijk?
Op volwassenheidsniveau 3 is IBP niet langer afhankelijk van individuele inspanningen, maar een gestandaardiseerd en geaccepteerd onderdeel van de organisatiecultuur. Dit maakt het eenvoudiger om risico's te beheersen, audits te doorstaan en te voldoen aan wet- en regelgeving zoals de AVG.

2. 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.

3. 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 om informatiebeveiliging en privacy binnen Stichting Akkoord!PO te regelen en is de kapstok voor de onderliggende afspraken en procedures.

4. Doel en reikwijdte

4.1 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 Stichting Akkoord 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 Akkoord voldoet aan relevante wet- en regelgeving.

4.2 Reikwijdte

- Het IBP-beleid binnen Stichting Akkoord!PO 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 Akkoord!PO waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting Akkoord!PO persoonsgegevens verwerkt.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting Akkoord!PO. Hieronder valt tevens de gecontroleerde informatie, die door een 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 Stichting Akkoord!PO 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 Akkoord!PO 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

5. Beleid – Hoe doen we dat?

Stichting Akkoord hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Stichting Akkoord!PO 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 Akkoord!PO voldoet aan alle relevante wet- en regelgeving.

3. Bij Stichting Akkoord!PO 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 Akkoord!PO 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 Akkoord!PO 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. Stichting Akkoord!PO legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Stichting Akkoord!PO voldoet hiermee aan de documentatieplicht.

6. Binnen Stichting Akkoord!PO 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 Akkoord!PO is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de stichting informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. Stichting Akkoord!PO 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. Stichting Akkoord!PO 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 Akkoord!PO 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 Akkoord!PO heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij Stichting Akkoord!PO een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. Stichting Akkoord!PO kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe informatiesystemen vooraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. Stichting Akkoord!PO 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 Stichting Akkoord!PO aanvullende afspraken vast over de technische maatregelen.

14. Stichting Akkoord!PO zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en, indien er risico's zijn voor de betrokkenen, melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

6. 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.

6.1 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
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- 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.

6.2 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 de overeenkomst, wettelijke verplichting, vitaal belang van betrokkene of andere personen, algemeen belang 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 (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiair). 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.

6.3 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.

6.4 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 o.a. bewustwordingscampagnes voor medewerkers. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP en de FG, met het bestuur als eindverantwoordelijke.

6.5 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.

6.6 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 datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij het Meldpunt Datalek Akkoord!PO via datalek@akkoord-po.nl.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

6.7 Planning en controle

Dit IBP-beleid wordt jaarlijks getoetst en bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

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

Daarnaast kent Stichting Akkoord!PO 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.

6.8 Logging en monitoring

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

7. Organisatie - Wie doet wat?

7.1 Rollen en verantwoordelijkheden (governance)

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 Akkoord!PO.

Richtinggevend	**Eindverantwoordelijk**	
	Verwerkingsverantwoordelijke : Voorzitter College van Bestuur	• *Eindverantwoordelijk* • *IBP-beleidsvorming, -vastlegging en communiceren ervan* • *Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens* • *Organisatie IBP inrichten; toewijzen van de taken en rollen* • *Evalueren toepassing en werking IBP-beleid op basis van rapportages*
Sturend	**Uitwerken beleid / inhoudelijk verantwoordelijk**	
	Privacy officer	• *Voorbereiden opstellen IBP-beleid, Classificatie/risicoanalyse* • *Inhoudelijk verantwoordelijk voor uitwerking van het IBP-beleid* • *Adviseert verwerkingsverantwoordelijke (bestuur/CvB/directie) over IBP* • *Uitwerken algemeen IBP-beleid naar specifiek beleid op een uniforme manier* • *Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering van het IBP-beleid te ondersteunen* • *Evalueren van het IBP-beleid en de maatregelen*
	Functionaris voor gegevensbescherming	• *Toezicht houden op naleving privacy wetgeving* • *Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens* • *Voorlichting privacy geven en stimuleren van bewustwording* • *Afwikkeling IBP klachten en incidenten*
	Afdelingshoofden Denk aan afdeling ict, P&O / HRM, facilitair, onderwijs, financiën administratie	• *Risicoanalyse in samenwerking met inhoudelijk verantwoordelijke* • *Toegangsbeleid zowel fysieke toegang als digitale toegang vaststellen en laten goedkeuren door de verwerkingsverantwoordelijke* • *Regelmatig de (netwerk)toegangsrechten van gebruikers beoordelen, controleren en vastleggen.*
Uitvoerend	**Uitvoeren beleid / naleven beleid**	
	• Privacy officer, ICT-beheerder • Privacy, functioneel beheer, applicatiebeheer • Alle medewerkers	• *Incidentafhandeling (registreren en evalueren).* • *Technisch aanspreekpunt voor IBP-incidenten.* • *Uitvoeren taken conform gegeven richtlijnen en procedures.* • *Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.*
	Toezicht naleving en communicatie	
	• FG • dagelijkse leiding, leidinggevende, directie	• *Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan.* • *Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers.* • *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.;*
	Opmerking: *in een aantal gevallen is ook de (G)MR hierbij betrokken.*	

De verdere uitwerking van de rollen en taken staan beschreven in bijlage 2.

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een opsomming van een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht. De beleidsstukken worden separaat aan dit beleidsplan aangeboden

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)
● Wachtwoordbeleid	
● Gedragscode ict en internetgebruik	
● Acceptable use policy	(verantwoord gebruik bedrijfsmiddelen)
● Procedure rondom uitwisselen gegevens	(passend onderwijs, leerlingdossiers, leerplicht e.v.)

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 voor Gegevensbescherming (communicatie hierover richting medewerkers)

Bijlage 2: Organisatie; wie doet wat (governance)

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 Akkoord!PO 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
De voorzitter 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 zal jaarlijks worden geëvalueerd. De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de Privacy Officer.

Sturend

Privacy Officer
De rol van Privacy Officer is sturend. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (voorzitter CvB) en stuurt de mensen aan op uitvoerend niveau. De Privacy Officer moet:
- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele stichting
- De uniformiteit bewaken binnen Stichting Akkoord!PO
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen Stichting Akkoord!PO coördineren

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG), houdt binnen Stichting Akkoord!PO 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 Privacy Officer. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Privacy Team en proceseigenaren
Binnen de school/het IKC/OKC zijn er verschillende domeinen/processen, zoals ICT, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies. Op school/IKC/OKC-niveau is de leidinggevende verantwoordelijk voor de risico's die veroorzaakt worden doordat personen (of applicaties) ten onrechte toegang krijgen tot applicaties. Hierbij wordt de leidinggevende ondersteund door leden van het Privacy Team.

Om deze risico's te verkleinen hebben proceseigenaren en leidinggevenden de volgende specifieke taken:

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

Uitvoerend

ICT-er en IT-Beheer (Cloudwise)
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 domeinverantwoordelijke / proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.
.
Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden worden beschreven in o.a. het personeelshandboek. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund door het Privacy Team en met bewustwordingsmateriaal (bijv. checklists en posters). 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(G) 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.
- 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 Privacy Officer en Privacy Team. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.