

Naam	Stichting samenwerkend bestuur KyK te Sneek (hierna: KyK Scholen)
Van	Voorzitter CvB
Aan	Alle betrokkenen
Datum	10 juli 2023
Betreft	Informatiebeveiligings- en privacy beleid (IBP)
Document	YSKN 11001 – V1.2 100723
Bron	Kennisnet

Formele versie gericht op compliance

Het informatiebeveiligings- en privacy beleid is aangepast aan de eisen en termen vanuit de AVG. Elke organisatie moet niet alleen de privacy wetgeving naleven, maar moet ook aantoonbaar voldoen aan de AVG.

Bij het template hoort een document met dezelfde inhoud, maar dan voorzien van een aparte toelichting. Die toelichting bevat verdere uitleg en verwijzingen naar onderliggende documenten, afspraken en procedures. Hiermee wordt de 'kapstokfunctie' van het beleid inzichtelijker.

Bron

Kennisnet

Bewerkt door:

Luuk Nicolai

Versie	Status	Datum	Auteur	Omschrijving
1.2		100723	Luuk Nicolai	Tweede conceptversie IBP-beleid

Vastgesteld door

Versie	Datum	Naam	Functie
		B. ten Kate	Voorzitter CvB

IBP regel je per schoolbestuur. Vaak zal IBP dan ook bovenschools geregeld worden. De heer B. ten Kate kan vervangen worden door de naam van de overkoepelende instelling.

1	HET BELANG VAN INFORMATIEBEVEILIGING EN PRIVACY	4
2	TOELICHTING INFORMATIEBEVEILIGING EN PRIVACY	4
2.1	TOELICHTING INFORMATIEBEVEILIGING	4
2.2	TOELICHTING PRIVACY	4
2.3	VERVLECHTING INFORMATIEBEVEILIGING EN PRIVACY	4
3	DOEL EN REIKWIJDTE	5
3.1	DOEL	5
3.2	REIKWIJDTE.....	5
4	BELEID – HOE DOEN WE DAT?	6
5	UITWERKING VAN HET BELEID – WAT DOEN WE?	8
5.1	RELEVANTE WET- EN REGELGEVING	8
5.2	BASISREGELS BIJ HET OMGAAN MET PERSOONSGEGEVENS.....	8
5.3	ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES	9
5.4	VOORLICHTING EN BEWUSTZIJN.....	9
5.5	CLASSIFICATIE EN RISICOANALYSE.....	9
5.6	INCIDENTEN EN DATALEKKEN	9
5.7	PLANNING EN CONTROLE	9
5.8	NALEVING EN SANCTIES	10
5.9	LOGGING EN MONITORING	10
6	ORGANISATIE - WIE DOET WAT?	11
6.1	ROLLEN EN VERANTWOORDELIJKHEDEN	11
	BIJLAGE 1: ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES	13
	BIJLAGE 2: ORGANISATIE; WIE DOET WAT	14

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 imagooverlies.

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 KyK Scholen 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 KyK Scholen 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 KyK Scholen voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen KyK Scholen geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreeerde) 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 KyK Scholen waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreeerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan KyK Scholen persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van KyK Scholen. 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 KyK Scholen 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 KyK Scholen raakvlakken met:
 - *Algemeen veiligheids- en toegangsbeveiligingsbeleid*; met als aandachtspunten bedrijfs-hulpverlening, 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?

KyK Scholen hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van KyK Scholen 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. KyK Scholen voldoet aan alle relevante wet- en regelgeving.
3. Bij KyK Scholen 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 KyK Scholen 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. KyK Scholen 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. KyK Scholen legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. KyK Scholen voldoet hiermee aan de documentatieplicht.
6. Binnen KyK Scholen 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. KyK Scholen 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. KyK Scholen 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. KyK Scholen 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. KyK Scholen 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 imagooverlies. KyK Scholen heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij KyK Scholen een continu proces, waarbij regelmatig

wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. KyK Scholen 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. KyK Scholen 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. KyK Scholen 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
- 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.

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.
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 privacy officer, de FG en de KyK-kring Bedrijfsvoering met het 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 de volgende e-mailadressen: sjouke.tjalsma@kykscholen.nl/fg@kykscholen.nl.

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

5.7 Planning en controle

Dit IBP-beleid wordt periodiek 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 KyK Scholen 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 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 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 voorzitter CvB, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door de voorzitter CvB vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan KyK Scholen 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 KyK Scholen.

Schema Rollen en Verantwoordelijkheden

Richtinggevend	Eindverantwoordelijk	
	Voorzitter CvB	<ul style="list-style-type: none"> 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	
	KyK-kring Bedrijfsvoering	<ul style="list-style-type: none"> Vorbereiden 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 (FG)	<ul style="list-style-type: none"> 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
	Proceseigenaren (te weten afdelingshoofd, beleidsadviseurs en schooldirecteuren)	<ul style="list-style-type: none"> 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	
	<ul style="list-style-type: none"> Privacy officer/beleidsadviseur ICT Functioneel beheerder, applicatiebeheerder Alle medewerkers 	<ul style="list-style-type: none"> 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	
Toezichhouders <ul style="list-style-type: none"> • FG • Privacy officer/beleidsadviseur ICT • College van Bestuur, Raad van Toezicht 	<ul style="list-style-type: none"> • <i>Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan.</i> • <i>Toeziën op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers.</i> • <i>Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid.</i> • <i>Implementeren IBP-maatregelen.</i> • <i>Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;</i>
Opmerking: <i>in een aantal gevallen is ook de (G)MR hierbij betrokken.</i>	

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:

Procedure toestemming gebruik beeldmateriaal
Procedure voor verwijderen van gegevens
Communicatie rechten betrokkenen
Procesbeschrijving rechten betrokkenen
Privacyreglement
Autorisatiematrix
Afspraken gebruik sociale media
Procedure rondom training medewerkers
Cameratoezicht
Wachtwoordbeleid
Responsible disclosure
Gedragscode ict en internetgebruik
Acceptable use policy
Procedure rondom uitwisselen gegevens

Aandachtspunten:

(toestemmingsbrief)
(bewaartermijnen)
(communicatie richting betrokkenen)
(proces rondom aanvragen van betrokkenen)

(wie mogen gegevens inzien, bewerken enz.)

(bewustzijn creëren)

(verantwoord gebruik bedrijfsmiddelen)
(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)
Risikoanalyse
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 KyK Scholen 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

Voorzitter CvB

De voorzitter CvB 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 privacy officer.

Sturend

KyK-kring Bedrijfsvoering

Deze groep houdt zich op sturend niveau bezig met alles rondom IBP. De KyK-kring Bedrijfsvoering bestaat uit de volgende leden:

- Beleidsadviseurs financiën, huisvesting, facilitair en ICT
- Functionaris gegevensbescherming
- Uitvoerende kwartiermaker (extern a.i.)

De KyK-kring Bedrijfsvoering heeft verder de volgende opdracht:

- Het signaleren en registreren van alle privacy verzoeken, beveiligingsincidenten en datalekken. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot incidenten hebben geleid of waardoor de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- Het leveren van managementrapportages en verbetervoorstellen aan de domeinverantwoordelijke/proceseigenaren over de beveiligingsincidenten en verzoeken tot uitoefening privacy-rechten van de betrokkenen.

Bij een calamiteit kan de KyK-kring Bedrijfsvoering terstond bij elkaar worden geroepen in opdracht van KyK Scholen. Het doel hiervan is om de **continuïteit** van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

- Datalek;
- Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
- Natuurrampen (brand, overstroming, storm, etc.).

De KyK-kring Bedrijfsvoering behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident. De werkzaamheden van de KyK-kring Bedrijfsvoering zijn gedocumenteerd en door de voorzitter CvB bekrachtigd.

Functionaris voor Gegevensbescherming

De functionaris gegevensbescherming (FG) houdt binnen KyK Scholen 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.

Proceseigenaren (hieronder vallen afdelingshoofden, beleidsadviseurs en schooldirecteuren)

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

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

- Samen met de voorzitter CvB/bovenschoolse ICT stellen zij het beleid voor toegang (autorisaties) vast.
- 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.

Uitvoerend

Privacy officer

De privacy officer (beleidsadviseur ICT) is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De privacy officer moet:

- het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling;
- de uniformiteit bewaken binnen KyK Scholen;
- het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy;
- de verdere afhandeling van incidenten binnen KyK Scholen coördineren, te weten:
- privacyverzoeken, beveiligingsincidenten en datalekken signaleren en registreren;
- daaropvolgende maatregelen coördineren;
- toezien op de oplossing van problemen die tot incidenten hebben geleid;
- managementrapportages en verbetervoorstellen leveren aan de proceseigenaren over beveiligingsincidenten en verzoeken van betrokkenen m.b.t. hun privacyrechten.

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

proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Medewerkers

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. de gedragscode voor veilig gebruik van ICT. 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).

Toezichthouders (hier: combinatie van FG, privacy officer, CvB en RvT)

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere toezichthouder 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.

De toezichthouder kan in zijn taak ondersteund worden door de privacy officer. Toezichthouders hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.