



Kon. Julianaschool

Leren om te Leven

Informatiebeveiligings- en privacy beleid

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.

Het uitgangspunt voor dit document vormt het template IBP beleidsdocument dat opgesteld is door het samenwerkingsverband PO raad / VO raad / Kennisnet. Bron Kennisnet

Bewerkt door:

Kon. Julianaschool

Vastgesteld door Kon. Julianaschool

Versie	Datum	Naam	Functie
1.0	17 mei 2018	Bestuur Kon.Julianaschool	bestuur

Inhoud

1 3

2 3

2.1 3

2.2 3

2.3 3

3 4

3.1 4

3.2 4

4 5

5 6

5.1 6

5.2 6

5.3 7

5.4 7

5.5 7

5.6 7

5.7 8

5.8 8

5.9 8

6 9

6.1 9

BIJLAGE 1: ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES

12

BIJLAGE 2: ORGANISATIE; WIE DOET WAT

13

1. Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van 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 de Kon. Julianaschool 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 Kon. Julianaschool 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 Kon. Julianaschool voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

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

4. Beleid – Hoe doen we dat?

Kon. Julianaschool hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. De Kon. Julianaschool 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. Bij Kon. Julianaschool 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 Kon. Julianaschool 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 ten alle tijden hun toestemming herzien.
3. Kon. Julianaschool zal alle betrokkenen helder en actief informeren over verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
4. Kon. Julianaschool legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Kon. Julianaschool voldoet hiermee aan de documentatieplicht.
5. Binnen Kon. Julianaschool 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.
6. Kon. Julianaschool 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 geïnformeerd over de regelgeving rondom het gebruik van informatie.
7. Kon. Julianaschool weegt de risico's die samenhangen met informatieverwerking en privacy en zoekt een balans tussen het afdekken van deze risico's en de daarvoor benodigde investeringen en de te nemen maatregelen.
8. Kon. Julianaschool 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.
9. Kon. Julianaschool verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Kon. Julianaschool heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
10. Informatiebeveiliging en privacy is bij Kon. Julianaschool een continu proces, waarbij regelmatig (minimaal 2- jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

11. Kon. Julianaschool 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.
12. Kon. Julianaschool 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.
Waar de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt Kon. Julianaschool aanvullende afspraken vast over de technische maatregelen in met derden afgesloten verwerkersovereenkomsten.
13. Kon. Julianaschool zal beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en waar van toepassing volgens de wet AVG 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

Bij de uitwerking van het beleid is het voldoen aan de volgende wetten en regels een uitgangspunt:

- Wet op het primair onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- Leerplichtwet

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 (Kon. Julianaschool) 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 **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. de zes wettelijke grondslagen zijn:
 - Toestemming van de betrokken persoon.
 - De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
 - De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting.
 - De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.

- De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
- De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

3. **Dataminimalisatie:** bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie:** de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

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 alleen voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hierbij ook 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 schooldirecteuren met het bestuur als eindverantwoordelijke.

5.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie 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 datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij de directeur. Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7 Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en zonodig 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 Kon. Julianaschool 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 het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekortschieten, dan spreekt de Kon. Julianaschool de betrokken (verantwoordelijke) medewerkers hierop aan.

5.9 Logging en monitoring

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

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. In bijlage 2 staat welke verantwoordelijkheden en taken bij welke rollen horen bij Kon. Julianaschool.

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.

Verplicht vanuit de AVG:

Privacyreglement
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)

Documenten:

Aandachtspunten:

Onderstaande documenten worden in 2018 opgesteld en volledig gemaakt. Per 25-5-2018 zijn deze gedeeltelijk of deels in concept beschikbaar.

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)
Autorisatiematrix	(wie mogen gegevens inzien, bewerken enz.)
Afspraken gebruik sociale media	
Procedure rondom training medewerkers	(bewustzijn creëren)
Cameratoezicht	
Wachtwoordbeleid	
Responsible disclosure	
Gedragscodex ict en internetgebruik	
Acceptable use policy	(verantwoord gebruik bedrijfsmiddelen)
Procedure rondom uitwisselen gegevens	(passend onderwijs, leerling dossiers, leerplicht enz)

Bijlage 2: Organisatie; wie doet wat

Deze bijlage geeft een nadere beschrijving van de verschillende IBP taken verboden aan de functies binnen de Kon. Julianaschool .

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

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Kon. Julianaschool voor elk niveau rollen en taken toegewezen aan medewerkers in de bestaande organisatie.

Richtinggevend

Eindverantwoordelijke

Het bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy op en vast. Ook stelt het bestuur het reglement voor de Functionaris Gegevensbescherming.

De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd. De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de directeuren van de scholen.

Toetsend / adviserend

Functionaris voor Gegevensbescherming of Privacy Officer

De functionaris voor gegevensbescherming (FG) houdt binnen Kon. Julianaschool 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 adviseert over verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, 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 directeuren. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Sturend / Uitvoerend

Directeuren scholen

Directeuren van de scholen zijn verantwoordelijk voor de uitvoering van het IBP beleid op de scholen.

- Initieert de periodieke beleidscyclus voor het actualiseren van het IBP beleid
- Rapporteert het bestuur over de uitvoering en evaluatie van het IBP beleid
- Voert risico analyses uit
- Vertaalt het beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- Is aanspreekpunt voor incidenten op het gebied van informatiebeveiliging en privacy
- Coördineert de afhandeling van incidenten binnen Kon. Julianaschool

De verdere taken en rollen van de directeur is:

- Er voor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid

- Stimuleren van veilig gedrag op het gebied van informatiebeveiliging en privacy
- Toezien op de uitvoering van vastgestelde maatregelen, richtlijnen en procedures
- Aanspreekpunt bij de afhandeling van incidenten binnen haar school (of scholen)
- Toezien 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.
- Bijdragen aan risico analyses
- Zorgen voor correcte uitvoering van de maatregelen voor toegangsbeveiliging en toegangsrechten tot applicaties of handmatige lijsten met privacy gevoelige gegevens.

(Meerscholen) directeuren kunnen onderdelen van deze taken delegeren aan medewerkers binnen de scholen (bijvoorbeeld medewerkers administratieve ondersteuning) maar blijven verantwoordelijk. (Meerscholen) directeuren worden ondersteund door de manager IBP bij de uitvoering van haar taken op het gebied van IBP.

Uitvoerend

Functioneel beheerder of Applicatiebeheerder

Ieder softwarepakket of (web-)applicatie heeft een (externe) beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De beheerder ontvangt van de directeur (applicaties per school) instructies en verzoeken voor het uitvoeren van de taken.

Teamleiders / Leerkrachten / IB-ers / Medewerkers

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in de vorm van maatregelen, instructies, checklists, formulieren of richtlijnen. Deze zijn opgenomen in het handboek van de Kon. Julianaschool .

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten bij de directeur, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR)

Extern ICT beheer

- Verantwoordelijk voor het correct uitvoeren van technische en procedurele maatregelen ter bescherming (privacy gevoelige) gegevensverwerking.
- Eerste aanspreekpunt voor het melden van ICT incidenten (opname bij de servicedesk)

Incident management

Er is een protocol waarin beschreven staat hoe te handelen bij (ernstige) beveiligingsincidenten. Afhankelijk van de ernst van het incident zijn achtereenvolgens (escalerend) de volgende functies betrokken:

- Medewerker: incident melding
- Extern ICT beheer: incident afhandeling en zo nodig escalatie naar directeur
- Directeur: incident afhandeling en zo nodig escalatie naar FG
- FG: zonodig melding AP en monitoring / advisering incident afhandeling
- Het bestuur: afhandeling incident en zo nodig contact met AP en/of betrokkene