# Informatiebeveiligings- en privacy beleid (IBP) Winkler Prins 2018

**Versie 17 september 2018**

Winkler Prins
openbare school voor voortgezet onderwijs

## 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.
Dit document beschrijft het IBP-beleid zoals dat binnen Winkler Prins in ontwikkeling is. De komende jaren zal op basis van verworven expertise, voortschrijdend inzicht en mogelijk veranderende wetgeving het IBP-beleid doorontwikkeld en aangepast gaan worden. Voor nu vormt dit IBP-plan de basis, de kapstok om processen, richtlijnen en procedures rondom IBP en de communicatie eromheen de komende tijd verder uit te werken en vast te leggen.

## 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 school. Incidenten en inbreuken in deze processen kunnen leiden tot schending van de privacy van betrokkenen, 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 Winkler Prins te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

## 3. Doel en reikwijdte

### 3.1 Doel

Informatiebeveiliging en privacy hebben de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Stichting Winkler Prins persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het 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 Winkler Prins voldoet aan relevante wet- en regelgeving.

### 3.2 Reikwijdte

- Het IBP-beleid binnen Stichting Winkler Prins geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing). Onder dit beleid vallen ook alle devices van waar toegang tot het schoolnetwerk verkregen kan worden alsmede alle geautoriseerde fysieke toegangen, deuren, kasten e.d.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting Winkler Prins waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting Winkler Prins persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen die vallen onder de verantwoordelijkheid van Stichting Winkler Prins. 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 Stichting Winkler Prins 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.
- Binnen Stichting Winkler Prins heeft het IBP-beleid raakvlakken met o.a.:
  - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.
  - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
  - *ICT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen.
  - *Informatiemanagement;* beleid op het gebied van opslag, beheer, bewerken van digitale gegevens in de systemen van Winkler Prins.
  - *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers.

## 4. Beleid – Hoe doen we dat?

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

1. Stichting Winkler Prins neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy goed geregeld zijn. De bestuurder is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is de bestuurder de verwerkingsverantwoordelijke.
2. Stichting Winkler Prins voldoet aan alle relevante wet- en regelgeving.
3. Bij Stichting Winkler Prins 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 Winkler Prins 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 Winkler Prins 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 Winkler Prins legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze actueel houden. Stichting Winkler Prins voldoet hiermee aan de documentatieplicht.
6. Binnen Stichting Winkler Prins 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 Winkler Prins 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. Stichting Winkler Prins classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er wordt een balans gezocht tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.
9. Stichting Winkler Prins 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 Winkler Prins verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zorgvuldig omgaan met hun verantwoordelijkheden, ook op het gebied van informatiebeveiliging en privacy. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Stichting Winkler Prins heeft hiervoor een Integriteitscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy bij Stichting Winkler Prins is een continu proces, waarbij regelmatig wordt geëvalueerd en wordt gekeken of aanpassing nodig of gewenst is.
12. Stichting Winkler Prins 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. Stichting Winkler Prins 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. Stichting Winkler Prins zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en indien nodig 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 voortgezet onderwijs
- Wet goed onderwijs, goed bestuur
- Wet op het onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Archiefwet

- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Onderwijsinstellingen en leveranciers geven invulling aan de eis van een op de AVG afgestemde verwerkersovereenkomst door gebruik te maken van het meest recente model verwerkersovereenkomst (medio 2018: versie 3.0). Deze Model Verwerkersovereenkomst is gepubliceerd op www.privacyconvenant.nl.

### 5.2 Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (AVG art.5) leidend. Deze zijn samengevat in vijf basisregels 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**: volgens de AVG artikel 6 is verwerking van persoonsgegevens alleen rechtmatig wanneer tenminste een van de hieronder genoemde wettelijke grondslagen van toepassing is:
   a. **Toestemming:** de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meerdere specifieke doeleinden. Wat hierbij van belang is, dat de betrokkene deze toestemming kan intrekken.
   b. **Overeenkomst:** de verwerking is noodzakelijk voor de uitvoering van een overeenkomst, waarbij de betrokkene partij is, of om op verzoek van de betrokkene voor de sluiting van een overeenkomst maatregelen te nemen. Denk hier bijvoorbeeld aan verwerking van persoonsgegevens in verband met de inschrijving van een leerling in de schooladministratie.
   c. **Wettelijke verplichting:** de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting, die op de verwerkingsverantwoordelijke rust. Bijvoorbeeld in geval van de plicht tot loonaangifte of een bewaarplicht Verwerking is dan noodzakelijk voor de nakoming van deze verplichting.
   d. **Vitaal belang:** de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen. Het redden van een leven is een rechtmatige grondslag voor het verwerken van persoonsgegevens. Het kan bijvoorbeeld gaan om het vastleggen van een allergie van een leerling.
   e. **Algemeen belang**: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.
   f. **Gerechtvaardigd belang**: de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. Privacybelang moet bij deze grondslag dus worden afgewogen tegenover belangen van de verwerkingsverantwoordelijke of derden. De verordening verwijst hier dus nog uitdrukkelijk naar situaties, waarbij betrokkene een kind is.
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 (subsidair). 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. De komende tijd zullen deze worden uitgewerkt. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en bijgehouden 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 inspanningsverplichting van de diverse verantwoordelijke functionarissen op het terrein van IBP, de Functionaris Gegevensbescherming (FG), met de bestuurder als werkingsverantwoordelijke.

## 5.5 Classificatie en risicoanalyse

Alle informatie heeft waarde en 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 datalekken. Alle beveiligingsincidenten worden vastgelegd in een incidentenregister. 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 bijgesteld door de bestuurder. Hierbij wordt rekening gehouden met:

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

Daarnaast vinden regelmatig overleg- en evalatiemomenten op operationeel, tactisch en strategisch niveau plaats.

## 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 bijvoorbeeld bij de aanstelling, tijdens functioneringsgesprekken, met periodieke bewustwordingscampagnes.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de bestuurder en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door de bestuurder vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan Stichting Winkler Prins 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 afdeling ICT zorgt ervoor 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?

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.
Dit hoofdstuk beschrijft hoe IBP op drie niveaus wordt georganiseerd en welke verantwoordelijkheden en taken bij welke rollen horen binnen Stichting Winkler Prins.
Er wordt onderscheid gemaakt tussen drie niveaus:

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

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Stichting Winkler Prins voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

### 6.1 Richtinggevend

**Verwerkingsverantwoordelijke**
De verwerkingsverantwoordelijke (bestuurder) is eindverantwoordelijk voor het IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.

### 6.2 Sturend

**Functionaris IBP**
De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de functionaris IBP. De functionaris IBP is een rol op sturend niveau. Hij geeft terugkoppeling en advies aan de verwerkingsverantwoordelijke (de bestuurder) en stuurt de mensen aan op uitvoerend niveau. De functionaris IBP heeft als taak:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling;
- De uniformiteit bewaken binnen Stichting Winkler Prins;
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy;
- De verdere afhandeling van incidenten binnen Stichting Winkler Prins coördineren.

**Functionaris voor Gegevensbescherming**
De functionaris voor gegevensbescherming (FG) houdt binnen Stichting Winkler Prins 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 verwerkingsverantwoordelijke. De FG heeft regelmatig overleg met functionaris IBP. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

**Stafdirecteur ICT**
De stafdirecteur ICT adviseert samen met functionaris IBP de verwerkingsverantwoordelijke. Hij is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen Stichting Winkler Prins.

**Domeinverantwoordelijken**
Binnen de school zijn er verschillende domeinen, zoals ICT, Facilitair, HR/PSA en leerlingadministratie. Op elk van deze domeinen is een medewerker verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.
Deze domeineigenaar is veelal een (staf)directeur. Hij 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 de domeineigenaren de volgende specifieke taken:

- Samen met de functionaris IBP en de stafdirecteur ICT doen zij voorstellen voor het beleid voor toegang tot de applicaties (autorisaties).
- 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.

## 6.3 Uitvoerend

**Functionaris IBP**
De Functionaris IBP is het technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

**Functioneel beheerder**
Ieder softwarepakket of (web-)applicatie heeft een functioneel beheerder. Bij vragen over de software of applicatie kan deze functioneel beheerder hierop aangesproken worden. De functioneel beheerder wordt vanuit de domeinverantwoordelijken (veelal een stafdirecteur) voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert de functioneel beheerder zijn taken uit.

**Medewerker**
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen die reeds ontwikkeld zijn of nog ontwikkeld gaan worden. Van medewerkers wordt verwacht dat zij actief betrokken zijn bij informatiebeveiliging. Dit kan door te werken volgens de richtlijnen van het informatiebeveiligingsbeleid en alle afspraken die n.a.v. daarvan zijn gemaakt, melding te maken van security incidenten, het uitoefenen van invloed op het beleid bijvoorbeeld door het doen van verbetervoorstellen.

**Leidinggevende**
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende 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 zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, functioneringsgesprekken, etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de functionaris IBP.

# 7. Tot slot

1. Het 'Informatiebeveiligings- en privacybeleid (IBP) Winkler Prins 2018' is vastgesteld door het bevoegd gezag van Winkler Prins op 16 oktober 2018 nadat de medezeggenschapsraad van Winkler Prins heeft ingestemd met het beleid in de vergadering van 15 oktober 2018.
2. Het bevoegd gezag stelt alle belanghebbenden op de hoogte van dit beleid.
3. Het beleid is via www.winklerprins.nl te downloaden of op verzoek bij een lid van het managementteam van de school op te vragen.
4. Het beleid kan door het bevoegd gezag worden gewijzigd of ingetrokken, met inachtneming van de geldende bepalingen.