Privacy (IBP) en veiligheidsbeleid
Stichting Spaarnesant
2018

Haarlem, 8 oktober 2018

open
baar
onder
wijs
Spaarne
sant

Inhoudsopgave

1

1. Inleiding en samenvatting 3

2. Functies en partners in het kader van de veiligheid 4

3. Informatiebeveiliging en Privacy, IBP 7

3.1. Begrippen in dit kader: 7

3.2. Privacy 8

3.3. Doel en reikwijdte 8

Doel 8

Reikwijdte 8

4. Ons beleid 9

4.1. Uitgangspunten IBP 9

Afspraken binnen Spaarnesant: 11

4.2. Basisregels bij het omgaan met persoonsgegevens 11

4.3. Planning en controle 12

4.4. Organisatie; wie doet wat 12

Eindverantwoordelijke 12

Directeur bedrijfsvoering 13

Functionaris voor Gegevensbescherming 13

Beleidsmedewerker/coördinator ICT 13

Proceseigenaar scholen 13

Functioneel beheerder of Applicatiebeheerder 13

Medewerker 14

Leidinggevende 14

Projectgroep 14

5. Informatiebeveiligingsincident en datalek 16

5.1. Wet- en regelgeving datalekken 16

Gebruikte begrippen: 16

5.2. Beleid Spaarnesant 17

5.3. Afspraken met leveranciers 17

6. Rechten van betrokkenen 17

7. Bijlage Privacyreglement Stichting Spaarnesant 18

8. Bijlage Formulier melding datalek door Verwerker 25

9. Bijlage CHECKLIST voor een AVG-PROOF werkplek!!! 30

10. Bijlage Beveiligd afdrukken instellen voor printer. 31

1. Inleiding en samenvatting

Op grond van de verschillende wetten heeft Spaarnesant als schoolbestuur de plicht privacy- en veiligheidsbeleid vast te stellen en in overleg met de scholen te implementeren in de organisatie. Het bestuur en de schoolleiding en personeel zijn samen verantwoordelijk voor de uitvoering van dit beleid. Voor Spaarnesant, dat al jaren met een veiligheidsbeleid werkt, betekent dit een aanvulling en aanpassing van het bestaande privacybeleid (IBP), voor het laatst vastgesteld in juni 2017, naar de nieuwste inzichten en eisen conform de Algemene Verordening Gegevensbescherming (AVG), die op 25 mei 2018 in werking treedt.

De door het bestuur van Spaarnesant ingestelde projectgroep AVG heeft de taak dit beleid in de periode maart 2018-maart 2020 voor te bereiden voor besluitvorming en te implementeren in de organisatie. Hierbij wordt gehandeld op basis van prioriteiten en met gebruikmaking van informatie en modellen, die onder andere zijn voorbereid door Kennisnet en de Autoriteit Persoonsgegevens.

Er is een uitgebreide informatietraject om de scholen hierop voor te bereiden en bewustwording te creëren, omdat de individuele werknemer de belangrijkste schakel is in de organisatie.
De schoolleiding en het personeel zorgen voor de uitvoering van het beleid op schoolniveau. Het Privacy- en Veiligheidsbeleid wordt in overleg met de (G)MR vastgesteld.

De Onderwijsinspectie ziet toe op naleving van deze wettelijke verplichtingen en let hierbij vooral op hoe de school vorm geeft aan het werken aan sociale veiligheid. Spaarnesant conformeert zich onder andere aan het waarderingskader 2017 van de inspectie voor het primair onderwijs. Verwacht wordt dat de accountant via de controleleidraad een taak krijgt in het kader van de controle van het privacybeleid. In het najaar van 2018 laat Spaarnesant een zgn. "PIA"[1] uitvoeren waardoor we kunnen vaststellen of we op de goede weg zijn.

Het privacy-reglement 2017 is nu aangepast aan de AVG en wordt breed onder de aandacht gebracht. Preventie en afhandeling van incidenten zijn ingebed in het pedagogisch beleid van de scholen en verankerd in de dagelijkse praktijk. De scholen maken gebruik van de protocollen en instrumenten die hiervoor beschikbaar zijn.

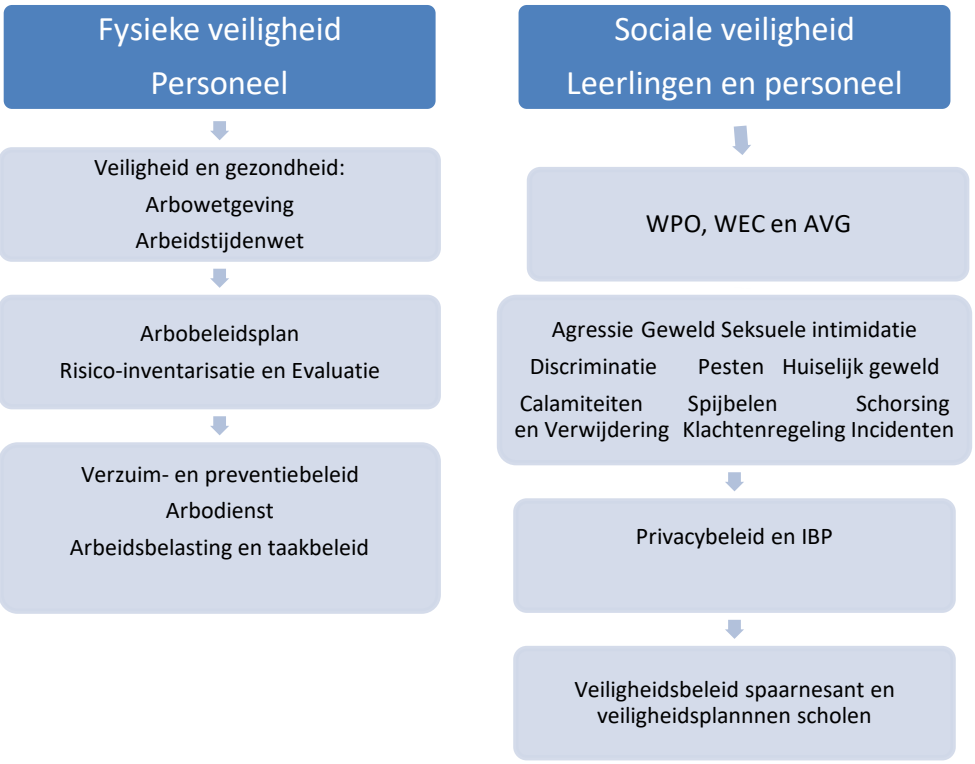
Uitgangspunten Spaarnesant:

- De schooldirectie en het personeel dragen zorg voor de privacy en de veiligheid van de school en haar omgeving gedurende de schooldag, voor alle leerlingen. Zij voorkomen datalekken, pesten, agressie en geweld in elke vorm en treden zo nodig snel en adequaat op.
- De schooldirectie, het personeel en de leerlingen gaan respectvol en betrokken met elkaar om. De leraren leren leerlingen sociale vaardigheden aan en tonen voorbeeldgedrag. Het veiligheidsbeleid is ingebed in het pedagogische beleid van de school en stevig verankerd in de dagelijkse praktijk. Ongewenst gedrag wordt voorkomen c.q. aangepakt.
- Het personeel van Spaarnesant conformeert zich aan en handelt volgens de door het bestuur in overleg met het personeel opgestelde gedragscode en geheimhoudingsverklaring.
- De school heeft veiligheidsbeleid, gericht op het voorkomen, registreren, afhandelen en evalueren van incidenten. Het beleid voorziet ook in een regelmatige meting van de veiligheidsbeleving van de leerlingen. De scholen hebben de functionarissen aangewezen die het aanspreekpunt zijn als het gaat om pesten of andere vormen van ongewenst gedrag.

[1] Een privacy impact assessment is een onderzoek waarbij wordt onderzocht wat de impact is het van project op de privacy van de betrokkenen, de risico's en de gevolgen.

In de navolgende hoofdstukken worden deze uitgangspunten verder uitgewerkt en aangevuld. Het is aan de scholen zelf om te laten zien hoe er actief wordt gewerkt aan bescherming van persoonsgegevens en sociale veiligheid (inspanningsverplichting) en welke effecten dat heeft voor de veiligheidsbeleving en het welbevinden van leerlingen (monitoring). Het is aan de scholen en de teams keuzes te maken, te bepalen wat werkt en welke afspraken passen.

Het begrip "veiligheid" is hierbij onder te verdelen in sociale veiligheid en fysieke veiligheid. Voorts is een onderverdeling te maken in veiligheid voor het personeel in het algemeen en voor de leerlingen op de scholen van Spaarnesant.



Het onderdeel fysieke veiligheid voor het personeel van Spaarnesant wordt vastgelegd in het Arbobeleidsplan dat in 2018 ook wordt geactualiseerd. Onderdeel hiervan zijn de zgn. "Risico Inventarisatie en Evaluaties"van de scholen en het bestuur. De RI&E wordt minimaal per vier jaar geactualiseerd. Spaarnesant gebruikt hiervoor de nieuwste digitale Arbomeester.
Nauw verwant met het veiligheidsbeleid is ook het begrip integriteit. Hiervoor heeft Spaarnesant in 2016 beleid vastgesteld, waaronder een klokkenluidersregeling.

De projectgroep maakt gebruik van een zgn. "Werkdocument AVG-1, dat als bijlage bij deze notitie is opgenomen.

2. Functies en partners in het kader van de veiligheid

Binnen het veiligheidsbeleid zijn verschillende taken binnen de school te onderscheiden:

Interne functies in de school	**Taak**

Directeur	Is namens het bestuur integraal verantwoordelijk voor de school en derhalve ook voor het veiligheidsbeleid
Preventiemedewerker/arbo-coordinator	Elke school heeft ten minste één preventiemedewerker in dienst hebben die de maatregelen (gericht op de veiligheid en gezondheid binnen de school) kan uitvoeren.
Vertrouwenspersoon/contactpersoon intern	Een interne vertrouwenspersoon of contactpersoon is er voor ouders, leerlingen en medewerkers die meldingen of klachten hebben over ongewenst gedrag zoals agressie en geweld, seksuele intimidatie/ongewenste intimiteiten, pesten en discriminatie
Bedrijfshulpverlener	Elke school treft maatregelen op het gebied van interne hulpverlening en stelt hiervoor een of meerdere medewerkers aan als bedrijfshulpverlener (BHV'er). Zij helpen in geval van ongevallen, brandbestrijding en evacuatie.
Intern beleleider	De intern begeleider organiseert, coördineert en bewaakt de leerlingenzorg binnen de school. Hij/zij ondersteunt leerkrachten bij het uitvoeren van zorgverbredingactiviteiten en zorgt voor afstemming van deze activiteiten op schoolniveau. Hij voert gesprekken met ouders en leerkrachten en ziet erop toe dat gemaakte afspraken met betrekking tot zorgleerlingen nageleefd worden. Daarnaast neemt de IB'er vaak toetsen af bij individuele kinderen en observeert hij soms in de groepen.
Anti-pest coördinator/coördinator sociale veiligheid	De anti pest coördinator is het eerste aanspreekpunt voor ouders en leerlingen bij pesten en coordineert het beleid waaronder het pestprotocol van de school; de coordinator sociale veiligheid is voor het brede beleid het aanspreekpunt.
Aandachtsfunctionaris huiselijk geweld en kindermishandeling	De aandachtfunctionaris is het aanspreekpunt voor ouders, leerlingen en leerkrachten en vormt de schakel met hulpverleningsinstanties. In gevallen van (het vermoeden van) huiselijk geweld en kindermishandeling hanteert de school de landelijke meldcode. Deze code geeft aan hoe scholen dienen te handelen bij het vermoeden van huiselijk geweld en kindermishandeling. Meestal wordt deze taak door de schooldirectie uitgevoerd.
Klachtenfunctionaris	Spaarnesant heeft een klachtenregeling
Externe functies rond de school	**Taak**
Vertrouwenspersoon extern	De externe vertrouwenspersoon kan worden ingeschakeld bij ongewenst gedrag. Meestal loopt dit via de interne contactpersoon
Klachtencommissie	In de klachtenregeling aangegeven dat Spaarnesant is aangesloten bij de Landelijke Klachtencommissie Onderwijs
Politie	Handhaving openbare orde
Leerplichtambtenaar	Handhaving leerplicht

Wijkteams voor gemeentelijke jeugdhulp / Centrum Jeugd en Gezin	Het CJG (Centrum voor Jeugd en Gezin) is een laagdrempelige voorziening waar iedereen terecht kan met vragen over opvoeden en opgroeien. Het bundelt de krachten van allerlei basisvoorzieningen die een taak hebben in de ondersteuning van ouders en jeugdigen (van 0 tot 23 jaar). Daarbij gaat het om gezondheid, ontwikkeling, opgroeien en opvoeden.
Schoolmaatschappelijk werk	Schoolmaatschappelijk werk is een laagdrempelige voorziening, aanwezig op school, welke erop gericht is om problemen vroegtijdig te signaleren en aan te pakken. Zij vervult een brugfunctie tussen kind, ouders, school en (jeugd-)zorginstellingen en richt zich op het kind bij wie de ontwikkeling stagneert. De begeleiding richt zich op degenen die invloed hebben op die situatie. Enerzijds zijn dit de ouders en verzorgers, anderzijds zijn dat bijvoorbeeld leerkrachten en de (jeugd-) hulpverlening.
Jeugd-GGZ	Jeugd ggz ondersteunt kinderen en jongeren met psychiatrische en psychische problemen en hun omgeving. Jeugd ggz helpt kinderen, jongeren en hun ouders met verschillende problemen. Samen wordt gekeken wat er aan de hand is en wordt gezocht naar een oplossing.
Slachtofferhulp	Slachtofferhulp Nederland helpt na een misdrijf**,** verkeersongeval, calamiteit of bij vermissing**.**
Verslavingszorg	Levert zorg bij verslaving bijvoorbeeld alcohol en drugs, internet of gokverslaving
Arbodeskundige	Een school moet zich laten bijstaan door een arbodeskundige, die adviezen geeft over het verbeteren van arbeidsomstandigheden en een zorgvuldige begeleiding van zieke werknemers. Dit doet bij Spaarnesant de arbo-arts. Een gecertificeerde arbodeskundige toetst de risico-inventarisatie en -evaluatie (RI&E).
Gemeente: Afdeling Leerplicht Wijkregisseur	 Handhaving leerplicht De wijkregisseur in de gemeente Haarlem heeft als taak de leefbaarheid in de wijk te bevorderen

Het veiligheidsbeleid van de scholen is uitgewerkt in de schoolveiligheidsplannen.

3. Informatiebeveiliging en Privacy, IBP

3.1. Begrippen in dit kader:

Privacy staat voor het recht om met rust te worden gelaten, het recht om te weten en te bepalen wat er met gegevens over jou gebeurt, en om te weten wie de beschikking heeft over jouw gegevens.

Onder **persoonsgegevens** verstaan we alle gegevens waarmee direct of indirect een natuurlijk persoon (mens) kan worden geïdentificeerd. Het kan bijvoorbeeld gaan om een naam, BSN-nummer, geboortedatum, telefoonnummer of IP-adres. Medewerkers- en leerling gegevens zijn ook persoonsgegevens.

De **betrokkene** is de mens over wie de persoonsgegevens gaan: in het po en vo is dit de leerling.Maar het kan ook gaan over de medewerker, de conciërge, OOP'er, leerkracht maar ook de directeur. Als de betrokkene jonger dan 16 jaar is, dan mogen volgens de AVG alleen de wettelijke vertegenwoordigers (ouders/verzorgers) beslissen over de gegevens van de betrokkene. De leerling beslist dan niet zelf.

Verantwoordelijke: een natuurlijke persoon of instantie (rechtspersoon), die vaststelt welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Het gaat hier om de persoon of instantie die formeel en juridisch het initiatief neemt tot het verzamelen van persoonsgegevens en daarvoor ook verantwoordelijk is. In het onderwijs is dit het bestuur van de rechtspersoon (stichting Spaarnesant) waar de school onder valt. Dit wordt aangegeven als het bevoegd gezag. Gemakshalve spreken we meestal over 'de school', maar dan bedoelen we dus het bevoegd gezag.

De ver**werker** is de leverancier voor de school die de persoonsgegevens van leerlingen of medewerkers verwerkt namens de verantwoordelijke. Dit is bijvoorbeeld een aanbieder van leermiddelen. De verwerker handelt in opdracht van de verantwoordelijke en mag alleen verwerkingen doen waarvoor hij uitdrukkelijk opdracht krijgt. Er is geen hiërarchische verhouding tussen de verantwoordelijke en de verwerker. Een verwerker is dus nooit in loondienst bij de verantwoordelijke.

Toezicht
In Nederland houdt de Autoriteit Persoonsgegevens (AP) toezicht op naleving van privacywet- en regelgeving. De AP kan boetes opleggen.

Register verwerkingsactiviteiten
Het register van verwerkingsactiviteiten bevat informatie over de persoonsgegevens die Spaarnesant verwerkt. Er staat onder andere in:

- De namen, functies en contactgegevens van de verantwoordelijke personen voor het IBP binnen Spaarnesant.
- Eventuele andere organisaties met wie Spaarnesant gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld.
- De Functionaris voor de gegevensbescherming (FG).
- Eventuele andere organisaties waarmee Spaarnesant persoonsgegevens deelt.
- De doelen waarvoor Spaarnesant de persoonsgegevens verwerkt. Bijvoorbeeld voor de werving en selectie van personeel, het bezorgen van producten of direct marketing;
- Een beschrijving van de categorieën van personen van wie Spaarnesant gegevens verwerkt. Bijvoorbeeld uitkeringsgerechtigden of klanten.

- Een beschrijving van de categorieën van persoonsgegevens. Zoals het BSN, NAW-gegevens, telefoonnummers, camerabeelden of IP-adressen.
- De datum waarop Spaarnesant de gegevens moet wissen (als dat/deze bekend is).
- De categorieën van ontvangers aan wie Spaarnesant persoonsgegevens verstrekt;
- Een algemene beschrijving van de technische en organisatorische maatregelen die Spaarnesant heeft genomen om persoonsgegevens die worden verwerkt te beveiligen.

3.2. Privacy

Privacy is een grondrecht. In Nederland is de privacybescherming tot 25 mei 2018 geregeld in de Wet bescherming persoonsgegevens (Wbp). Deze wet beschermt de privacy door regels te stellen voor de omgang met persoonsgegevens in Nederland. Op 25 mei 2018 is de Wbp vervangen worden door een Europese privacywet: de Algemene Verordening Gegevensbescherming (AVG).
Leerlinggegevens zijn ook persoonsgegevens[2] en vallen onder de AVG. Gevoelige persoonsgegevens mogen alleen worden vastgelegd door de scholen als dat noodzakelijk is. Denk hierbij aan informatie over gezondheid, gedragsproblemen, godsdienst of een problematische thuissituatie. Het vastleggen hiervan kan van belang zijn voor de speciale begeleiding van leerlingen of om bijzondere voorzieningen te kunnen treffen zoals registratie van allergieën of diabetes. In geval van nood kan dan de juiste procedure worden gevolgd. Wat ermee gedaan wordt heet **verwerken**, dus verzamelen, kopiëren, opslaan, verspreiden, publiceren en uitwisselen. 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.

3.3. Doel en reikwijdte

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 Spaarnesant 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 Spaarnesant voldoet aan relevante wet- en regelgeving.

Reikwijdte

- Het IBP-beleid binnen Spaarnesant geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing). Onder dit beleid vallen ook

[2] Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd.

alle devices van waar geautoriseerde toegang tot het (school)netwerk verkregen kan worden.

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

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Spaarnesant 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 Spaarnesant 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.

4. Ons beleid

4.1. Uitgangspunten IBP

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

1. Het schoolbestuur van Spaarnesant neemt de verantwoordelijkheid 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. Spaarnesant voldoet aan alle relevante wet- en regelgeving.

2. Bij Spaarnesant 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 Spaarnesant 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. Spaarnesant 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 (gegevens overdraagbaarheid) en profilering.

4. Spaarnesant legt alle verwerkingen van persoonsgegevens vast in een data of verwerkingsregister en zal deze up-to-date houden. Spaarnesant voldoet hiermee aan de documentatieplicht volgens de AVG.

5. Binnen Spaarnesant 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. Spaarnesant 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.

7. Spaarnesant 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 tenemen maatregelen.

8. Spaarnesant 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. Spaarnesant 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. Spaarnesant heeft hiervoor voor het eigen personeel een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

10. Informatiebeveiliging en privacy is bij Spaarnesant een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

11. Spaarnesant 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. Spaarnesant 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.

13. Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt Spaarnesant aanvullende afspraken vast over de technische maatregelen.

14. Spaarnesant zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens.

15. Bij Spaarnesant regelen de scholen in een procedure hoe betrokkenen hun rechten kunnen uitoefenen. Hierbij wordt gebruik gemaakt van de klachtenregeling, waarbij klagers in eerste instantie bij de directeur van de school terecht moeten met hun klachten. In de meeste gevallen kan voor de rechten van de betrokkene, dezelfde procedure worden doorlopen. Als de betrokkene jonger is dan 16 jaar, zijn alleen zijn wettelijk vertegenwoordigers bevoegd om een verzoek in te dienen.

16. Bij de Spaarnesant scholen is de schooldirecteur verantwoordelijk om klachten van betrokkenen te behandelen, behoudens de hiervoor aangestelde functionaris binnen of buiten de school.

Afspraken binnen Spaarnesant:

1. De medewerkers van Spaarnesant zijn op de hoogte van de uitgangspunten van privacybescherming en handelen hiernaar.
2. Naast het veiligheidsplan van het bestuur beschikt elke school over een (sociaal) veilgheidsplan en bijbehorende protocollen. Het bestuur heeft een "Spaarnesant privacyreglement" (bijlage) opgesteld dat ook geldt voor alle scholen/werknemers.
3. De scholen hebben de regie op wat er gebeurt met de persoonsgegevens van de leerlingen en het personeel van de school en gebruiken deze informatie binnen de kaders van de wet om het onderwijs te kunnen geven en organiseren. Hierbij houden zij rekening met de rechten van ouders en de MR en het bestuursbeleid.
4. De scholen zijn transparant over het verzamelen en het gebruiken van persoonsgegevens van en over de leerlingen en kunnen verantwoorden wat er met die gegevens gebeurt.
5. Voor het gebruik maken van herkenbare foto's en video's op school wordt vooraf schriftelijke toestemming gevraagd aan de ouders. Dit kan bij de inschrijving van de leerling, maar dit is gedurende de schoolloopbaan ook nodig als foto's worden gebruikt voor de website, nieuwsbrieven of voor social media. Scholen nemen dit op in de schoolgids en brengen dit jaarlijk sonder de aandacht van de ouders.
6. Bij de overstap naar een andere school, horizontaal (PO) of verticaal (VO), handelen onze scholen volgens het zgn. "overstapprotocol" dat vanuit de samenwerkingsverbanden PO en VO is opgesteld conform het "OSO", Overstapservice Onderwijs. Hierbij wordt het relevante onderwijskundig rapport digitaal overgedragen. Hierin staat de informatie die de nieuwe school nodig heeft om het onderwijs te kunnen overnemen. Ouders hebben ten allen tijde inzagerecht.
7. De persoonsgegevens binnen Spaarnesant worden beveiligd tegen risico's volgens de "stand der techniek". Hierbij gaat het om algemeen geaccepteerde en toegepaste organisatorische en technische beveiligingsnormen. Dit geldt zowel voor de scholen als voor de leveranciers. Er hebben niet meer medewerkers toegang tot (zeer) gevoelige informatie dan strikt nodig is. De bewaartermijn van persoonsgegevens is 2 jaar na vertrek van de leerling, tenzij de wet een andere termijn voorschrijft, zoals bij het bewaren van diploma's of 3 jaar voor een overstapdossier. De wettelijke bewaartermijnen voor personeelsgegevens worden in acht genomen.

4.2. 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 (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.

4.3. Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur. 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 neemt Spaarnesant de controle van IBP mee in de jaarlijkse planning en control cyclus. 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.

4.4. Organisatie; wie doet wat

Binnen Spaarnesant wordt de IBP op drie niveaus wordt georganiseerd:

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

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

Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Eindverantwoordelijke

Het schoolbestuur (College van Bestuur) is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd. De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de directeur bedrijfsvoering.

Sturend

Directeur bedrijfsvoering

De directeur bedrijfsvoering (DB) is verantwoordelijke voor de IBP en heeft een rol op sturend niveau. Hij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De DB moet:

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

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen Spaarnesant 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 nformatiebeveiligingsincidenten, 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 DB. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Beleidsmedewerker/coördinator ICT

Adviseert en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen Spaarnesant.

Proceseigenaar scholen

Binnen de scholen 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 de directeur verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies. Op basis van mandatering kunnen taken aan functionarissen binnen de school zijn overgedragen.

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 eindverantwoordelijke 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

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.

Medewerker

Alle medewerkers binnen Spaarnesant hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in de functiebeschrijving en protocollen. 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)

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, 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 leidinggevende kan in zijn taak ondersteund worden door de DB. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Projectgroep

Een AVG-projectgroep is organisatie breed benoemd voor de voorbereiding en informatieverstrekking van het IBP. De projectgroepleden zijn benoemd door de DB en handelen in diens opdracht.
De AVG projectgroep van Spaarnesant heeft de volgende opdracht:

- Het voorbereiden van het beleid, modellen, protocollen e.d. en de informatievertrekking binnen en buiten de stichting.
- 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 medewerkers, ouders, systeembeheerders, ontwikkelaars, leveranciers en eindgebruikers door het verspreiden van informatie;
- Het leveren van managementrapportages en verbetervoorstellen aan de DB en de schooldirecties/proceseigenaren over de beveiligingsincidenten en verzoeken tot uitoefening privacyrechten van de betrokkenen.

Bij een calamiteit kan de AVG groep terstond bij elkaar worden geroepen op initiatief van de DB, in opdracht van Spaarnesant. Het doel hiervan is om de **continuïteit** van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

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

De AVG projectgroep van Spaarnesant behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.

5. Informatiebeveiligingsincident en datalek

5.1. Wet- en regelgeving datalekken

Gebruikte begrippen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening**; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek**; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplichting melding te maken van ernstige datalekken bij de AP. Het nalaten van deze melding kan leiden tot een fikse boete. De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in de leerlingadministratie, digitale leermiddelen of de salarisadministratie. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan is of worden hiervoor via het bestuur met deze verwerkers aanvullende afspraken gemaakt over het melden van datalekken. Spaarnesant maakt hierbij gebruik van de afspraken die hiervoor landelijk voor de schoolbesturen zijn voorbereid.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie ‘gelekt’. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van een klas is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een vewerker voor de school. Er kan worden afgesproken dat een vewerker **namens** de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

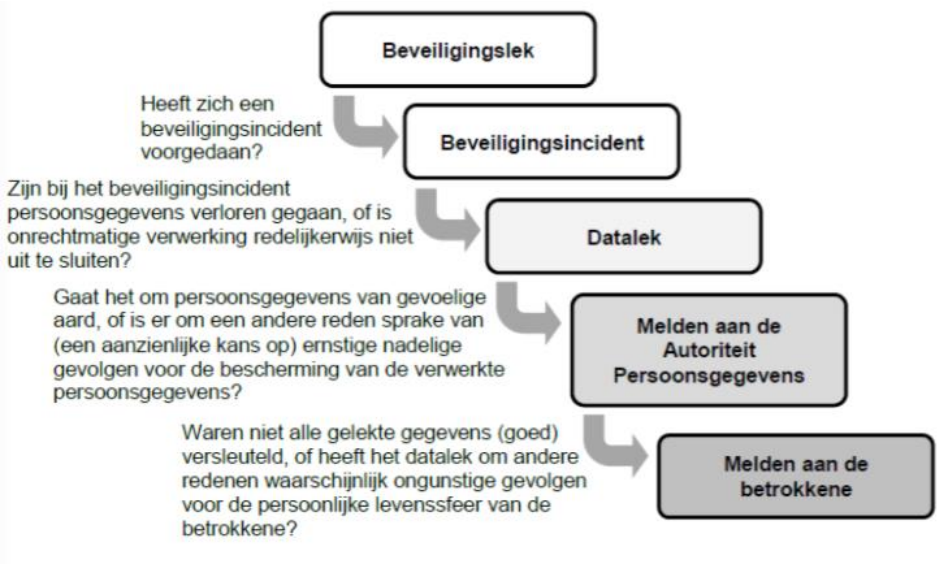
5.2. Beleid Spaarnesant

Spaarnesant scholen hebben in het veiligheidsbeleid geregeld dat zij informatie beveiligingsincidenten en datalekken melden bij het bestuur. Spaarnesant handelt volgens het model dat in de beleidsregels van de Autoriteit Persoonsgegevens hiervoor is vastgeld. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf Het protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is deze te voorkomen. Dit protocol is van toepassing op de gehele organisatie. Een meldingsformulier en mailadres "meldpuntdatalekken@spaarnesant.nl" is hiervoor vastgesteld (bijlage).

5.3. Afspraken met leveranciers

Spaarnesant maakt als verantwoordelijke voor de persoonsgegevens afspraken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder.
Hiervoor wordt gebruik gemaakt van de model verwerkingsovereenkomst (3.0)[3] die hoort bij het convenant "Digitale onderwijsmiddelen en privacy" (www.privacyconvenant.nl).

Na het ontdekken van een beveiligingsincident worden de volgende stappen genomen:



6. Rechten van betrokkenen

Indien het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van een betrokkene, dan melding dan meldt Spaarnesant dit ook aan de betrokkenen zelf. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). Als deze persoonsgegevens zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld.

[3] In een verwerkingsovereenkomst is vastgelegd dat de verwerkingsverantwoordelijke (schoolbestuur) aan een andere organisatie (een verwerker) een opdracht heeft verstrekt waarbij verwerking van persoonsgegevens aan de orde is.

7. Bijlage Privacyreglement Stichting Spaarnesant

Toepasselijkheid	Dit reglement geldt voor de gehele organisatie die deel uitmaakt van Stichting SPAARNESANT. SPAARNESANT is gevestigd aan de Schipholpoort 2, 2034 MA te Haarlem.
Definities	
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'), zoals bijvoorbeeld naam, adres, geboortedatum, titel(s), geslacht, adres, telefoonnummer, e-mailadres, functie, personeelsnummer, medische rapportages, inhoud van e-mails, prestaties/cijfers, brieven, klachten, foto's, video's, IP-adressen, tracking cookies, loginnamen en wachtwoorden.
Verwerking van persoonsgegevens	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, geautomatiseerd of handmatig, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Bijzondere persoonsgegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische gegevens (DNA/RNA) of biometrische gegevens (bijv. foto's) met het oog op de unieke identificatie van een persoon, en gegevens over gezondheid, of iemands seksueel gedrag of seksuele gerichtheid.
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft, en die al dan niet wordt vertegenwoordigd door een wettelijk vertegenwoordiger. Betrokkenen kunnen bijvoorbeeld zijn: leerlingen, ouders, medewerkers en bezoekers.
Wettelijk vertegenwoordiger	Degene die het ouderlijk gezag over een minderjarige uitoefent. Meestal zal dit een ouder zijn, maar het kan ook gaan om een voogd. Als een leerling 16 jaar of ouder is, beslist hij in voorkomende gevallen zelf over zijn privacy.
Verwerkings-verantwoordelijke	De entiteit die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit reglement is het Spaarnesant, te weten SPAARNESANT, vertegenwoordigd door het College van Bestuur, de verwerkingsverantwoordelijke.
Verwerker	De natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke SPAARNESANT persoonsgegevens verwerkt, zoals bijvoorbeeld de leverancier van een leerlingvolgsysteem of leerling-administratiesysteem. Een verwerker heeft een uitvoerende taak, ten behoeve van de activiteiten van de verwerkingsverantwoordelijke.
Derde	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, de verwerkingsverantwoordelijke, de verwerker, of de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om

	persoonsgegevens te verwerken.
SPAARNESANT	Stichting SPAARNESANT, de verwerkingsverantwoordelijke in de zin van dit reglement.
Reikwijdte en doelstelling	1. Dit reglement stelt regels over de verwerking van persoonsgegevens van alle betrokkenen bij de organisatie, waaronder leerlingen en hun wettelijk vertegenwoordigers, medewerkers, bezoekers en externe relaties (bijv. leveranciers en opdrachtnemers). 2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door de SPAARNESANT worden verwerkt. Het reglement heeft tot doel: a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens; b. vast te stellen met welk doel en op welke (juridische) grondslag persoonsgegevens binnen SPAARNESANT worden verwerkt; c. ook overigens te borgen dat persoonsgegevens binnen SPAARNESANT rechtmatig, transparant en behoorlijk worden verwerkt; d. de rechten van betrokkenen vast te leggen en te borgen dat deze rechten door SPAARNESANT worden gerespecteerd.
Doelen van de verwerking van persoonsgegevens	Bij de verwerking van persoonsgegevens houdt SPAARNESANT zich aan de relevante wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG), de uitvoeringswet AVG en de onderwijswetgeving.
Doelen	1. De verwerking van persoonsgegevens vindt plaats voor: a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, het voorzien in hun (extra) ondersteuningsbehoefte, dan wel het geven van studieadviezen; b. het verstrekken en/of ter beschikking stellen van leermiddelen; c. het bewaken van de veiligheid binnen de scholen en het beschermen van eigendommen van medewerkers, leerlingen en bezoekers; d. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld, onder a en b, alsmede van informatie over de leerlingen op de eigen website; e. het bekend maken van de activiteiten van de organisatie, bijvoorbeeld op de website van SPAARNESANT of van de scholen, in brochures of de schoolgids of via social media; f. het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen; g. het aanvragen van bekostiging, het behandelen van geschillen daarover en het doen uitoefenen van accountantscontrole; h. het onderhouden van contacten met oud-leerlingen; i. het aangaan en uitvoeren van arbeidsovereenkomsten, samenwerkingsrelaties met opdrachtnemers en contracten met leveranciers en het verwerken van de salarissen van de werknemers inclusief afdrachten van werkgever- en werknemerspremies en inhoudingen; j. de uitvoering of toepassing van wet- en regelgeving; k. juridische procedures waarbij SPAARNESANT betrokken is. 2. De verwerking van persoonsgegevens mag ook plaatsvinden voor doelen die verenigbaar zijn met de doelen zoals beschreven in lid 1.

Doelbinding	Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. SPAARNESANT verwerkt niet meer gegevens dan noodzakelijk is om de betreffende doelen te bereiken.
Soorten persoonsgegevens	De categorieën van persoonsgegevens zoals deze binnen SPAARNESANT worden verwerkt, worden geregistreerd in een verwerkingsregister.
Grondslag verwerking	Verwerking van persoonsgegevens gebeurt alleen indien aan een van de onderstaande voorwaarden is voldaan: 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 SPAARNESANT is opgedragen. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op SPAARNESANT rust. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de arbeidsovereenkomst) of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van SPAARNESANT of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen, met name wanneer de betrokkene een kind is; in het kader van deze grondslag zal dus een belangenafweging moeten plaatsvinden. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen (levensbelang). De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.
Bewaartermijnen	SPAARNESANT bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor deze worden verwerkt, tenzij het langer bewaren van de persoonsgegevens op grond van wet- of regelgeving verplicht is.
Toegang	Binnen de organisatie van SPAARNESANT geldt dat personen slechts toegang hebben tot persoonsgegevens voor zover dat daadwerkelijk nodig is. De toegang van medewerkers tot persoonsgegevens is dan ook beperkt tot de gegevens die noodzakelijk zijn voor de goede uitoefening van hun functie en (dus) hun werkzaamheden. Verder wordt slechts toegang verschaft tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan: a. de verwerker die van SPAARNESANT de opdracht heeft gekregen om persoonsgegevens te verwerken, maar alleen voor zover dat noodzakelijk is in het licht van de gemaakte afspraken; b. derden voor zover uit de wet voortvloeit dat SPAARNESANT verplicht is om toegang te geven of sprake is van een (andere) grondslag voor deze verwerking, bijvoorbeeld de vervulling van een taak van algemeen belang of afdracht van salarispremies en inhoudingen e.d..
Beveiliging en geheimhouding	1. SPAARNESANT neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden

	beschadigd, verloren gaan of onrechtmatig worden verwerkt. Deze maatregelen zijn er mede op gericht om niet noodzakelijke verzameling en verdere (niet noodzakelijke) verwerking van persoonsgegevens te voorkomen. 2. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen. 3. Een ieder die betrokken is bij de verwerking van persoonsgegevens binnen SPAARNESANT is verplicht tot geheimhouding van de betreffende persoonsgegevens, en zal deze gegevens slechts verwerken voor zover dat noodzakelijk is voor de uitoefening van de betreffende functie, werkzaamheden of taak. SPAARNESANT heeft hiervoor gedragscodes en geheimhoudingsverklaringen opgesteld voor werknemers in de school en voor het stafbureau. Bij indiensttreding conformeren werknemers zich hieraan.
Verstrekken gegevens aan derden	SPAARNESANT kan persoonsgegevens aan derden verstrekken als daarvoor een grondslag bestaat in de zin van artikel 7 van dit reglement.
Sociale media	Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het sociaal veiligheidsbeleid van SPAARNESANT.
Rechten betrokkenen	SPAARNESANT erkent de rechten van betrokkenen, handelt daarmee in overeenstemming en bewerkstelligt dat betrokkenen deze rechten daadwerkelijk kunnen uitoefenen. Het betreft in het bijzonder de volgende rechten:
Inzage	Een betrokkene heeft recht op inzage van de door SPAARNESANT verwerkte persoonsgegevens die op hem betrekking hebben, behalve voor zover het gaat om werkdocumenten, interne notities en andere documenten die uitsluitend bedoeld zijn voor intern overleg en beraad. Indien en voor zover dit recht op inzage ook de rechten en vrijheden van anderen raakt, bijvoorbeeld als in de documenten ook persoonsgegevens van anderen dan de betrokkene zijn vermeld, kan SPAARNESANT het recht op inzage beperken. Bij het verstrekken van de betreffende gegevens verschaft SPAARNESANT voorts informatie over: de verwerkingsdoeleinden; de categorieën van persoonsgegevens die worden verwerkt; de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt; (indien mogelijk) hoe lang de gegevens worden bewaard; dat de betrokkene het recht heeft om te verzoeken dat de persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van de persoonsgegevens wordt beperkt, alsmede dat hij het recht heeft om bezwaar te maken tegen de verwerking van de persoonsgegevens; het feit dat de betrokkene een klacht kan indienen bij de Autoriteit Persoonsgegevens; de bron van de persoonsgegevens, indien de persoonsgegevens niet van de betrokkene zelf zijn verkregen; het eventueel toepassen van geautomatiseerde besluitvorming en de betreffende onderliggende logica en het belang en de gevolgen voor de betrokkene; de passende waarborgen indien de persoonsgegevens worden doorgegeven.

Verbetering, aanvulling, verwijdering	SPAARNESANT verbetert de persoonsgegevens van een betrokkene in het geval de betrokkene terecht heeft aangegeven dat de gegevens onjuist zijn, en SPAARNESANT vult de persoonsgegevens van een betrokkene aan indien de betrokkene terecht om aanvulling heeft verzocht. Voorts kan de betrokkene verzoeken om verwijdering van zijn persoonsgegevens. SPAARNESANT gaat daartoe over indien is voldaan aan een wettelijke grondslag voor het verzoek, tenzij het onmogelijk is om aan het verzoek te voldoen of dit een onredelijke inspanning zou vergen.
Bezwaar	Indien SPAARNESANT persoonsgegevens verwerkt op de grondslag van artikel 7 onder a of artikel 7 onder d van dit reglement, kan de betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens. In dat geval staakt SPAARNESANT de verwerking van de betreffende persoonsgegevens, behalve als naar het oordeel van SPAARNESANT het belang van SPAARNESANT, het belang van derden of het algemeen belang in het betreffende concrete geval zwaarder weegt.
Beperken verwerking	De betrokkene kan voorts verzoeken om de verwerking van zijn persoonsgegevens te beperken, namelijk indien hij een verzoek tot verbetering heeft gedaan, indien hij bezwaar heeft gemaakt tegen de verwerking, als de persoonsgegevens niet meer nodig zijn voor het doel van de verwerking of als de gegevensverwerking onrechtmatig is. SPAARNESANT staakt dan de verwerking, tenzij de betrokkene toestemming heeft gegeven voor de verwerking, SPAARNESANT de gegevens nodig heeft voor een rechtszaak of de verwerking nodig is ter bescherming van de rechten van een andere persoon of vanwege gewichtige redenen.
Kennisgevingsplicht	Als SPAARNESANT op verzoek van een betrokkene een verbetering of verwijdering van persoonsgegevens heeft uitgevoerd, of de verwerking van persoonsgegevens heeft beperkt, zal SPAARNESANT eventuele ontvangers van de betreffende persoonsgegevens daarover informeren.
Procedure	SPAARNESANT handelt een verzoek van een betrokkene zo spoedig mogelijk, maar uiterlijk binnen een maand na ontvangst van het verzoek, af. Afhankelijk van de complexiteit en van het aantal verzoeken kan die termijn indien nodig met twee maanden worden verlengd. Als deze verlenging plaatsvindt, wordt de betrokkene daarover binnen een maand na de ontvangst van het verzoek geïnformeerd. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt. Wanneer SPAARNESANT geen gevolg geeft aan het verzoek van de betrokkene, deelt SPAARNESANT onverwijld en uiterlijk binnen een maand na ontvangst mede waarom het verzoek niet wordt ingewilligd en informeert hij de betrokkene over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of beroep bij de rechter in te stellen.
Intrekken toestemming	Indien voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijde door de betrokkene of zijn wettelijk vertegenwoordiger worden ingetrokken. Als de toestemming wordt ingetrokken, staakt SPAARNESANT de verwerking van persoonsgegevens, behalve als er een andere grondslag (zoals bedoeld in artikel 7) voor de gegevensverwerking is. Het intrekken van de toestemming tast de rechtmatigheid van verwerkingen die reeds hebben plaatsgevonden niet aan.

Transparantie	SPAARNESANT informeert de betrokkene(n) actief over de verwerking van hun persoonsgegevens, in ieder geval door middel van een laagdrempelige privacyverklaring. In de privacyverklaring wordt in ieder geval de volgende informatie vermeld: a) de contactgegevens van SPAARNESANT; b) de contactgegevens van de functionaris voor gegevensbescherming van SPAARNESANT; c) de doeleinden van de gegevensverwerking en de grondslagen voor de verwerking; d) een omschrijving van de belangen van SPAARNESANT indien de verwerking wordt gebaseerd op het gerechtvaardigd belang van SPAARNESANT; e) de (categorieën) ontvangers van de persoonsgegevens, zoals verwerkers of derden; f) in voorkomend geval: of de persoonsgegevens worden verzonden aan landen buiten de Europese Economische Ruimte (EER); g) hoe lang de persoonsgegevens zullen worden bewaard; h) dat de betrokkene het recht heeft om SPAARNESANT te verzoeken om inzage, verbetering of verwijdering van persoonsgegevens, en dat hij het recht heeft om te verzoeken om beperking van de verwerking, om bezwaar te maken of om een beroep te doen op het recht van gegevensoverdraagbaarheid; i) dat de betrokkene het recht heeft om zijn toestemming in te trekken, als de gegevensverwerking is gebaseerd op toestemming; j) dat de betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens; k) of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te kunnen sluiten, en of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de gevolgen zijn indien hij de persoonsgegevens niet verstrekt; l) het bestaan van geautomatiseerde besluitvorming, vergezeld van nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.
Meldplicht datalekken	Een ieder die betrokken is bij een verwerking van persoonsgegevens is verplicht om een datalek per ommegaande te melden bij het meldpunt van het bestuur, meldpuntdatalek@spaarnesant.nl, conform het protocol beveiligingsincidenten en datalekken van SPAARNESANT. Een datalek is elke inbreuk waarbij persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk zijn gemaakt.
Klachten	1. Wanneer een betrokkene van mening is dat het doen of nalaten van SPAARNESANT niet in overeenstemming is met de AVG, dit reglement of (andere) toepasselijke wet- of regelgeving, dan kan een klacht worden ingediend overeenkomstig de binnen SPAARNESANT geldende klachtenregeling. Een betrokkene kan zich eveneens wenden tot de functionaris voor gegevensbescherming van SPAARNESANT. 2. Als een klacht naar de mening van betrokkene door SPAARNESANT niet correct is afgewikkeld, kan hij zich wenden tot de rechter of de Autoriteit Persoonsgegevens.

Onvoorziene situatie	Indien zich een situatie voordoet die niet beschreven is in dit reglement, neemt het College van Bestuur van SPAARNESANT de benodigde maatregelen, en wordt beoordeeld of dit reglement dientengevolge moet worden aangevuld of aangepast.
Wijzigingen reglement	1. Dit reglement is met instemming van de Gemeenschappelijke Medezeggenschapsraad (GMR) vastgesteld door het College van Bestuur van SPAARNESANT. Het reglement wordt gepubliceerd op de website van SPAARNESANT en de websites van de scholen. Het reglement wordt verder actief onder de aandacht gebracht, bijvoorbeeld door middel van verwijzing in de schoolgids. 2. Het College van Bestuur kan dit reglement wijzigen na instemming van de GMR.
Slotbepaling	Dit reglement wordt aangehaald als het Privacyreglement van SPAARNESANT en treedt in werking op 8 oktober 2018 en vervangt het voorlopige Privacyreglement dat op 24 mei 2018 is vastgesteld.

8. Bijlage Formulier melding datalek door Verwerker

De melding wordt gedaan door de directie van de Verwerker aan Opdrachtgever. Updates van het vragenformulier worden telkens zo snel mogelijk aan de Opdrachtgever beschikbaar gesteld, genoemd aan het einde van dit formulier.

Vragenformulier melding

0) Contactpersoon bij Verwerker:

Vul onderstaande gegevens in:	
Naam:	Cindy Fatels
Functie:	FG
Mobiele telefoon:	023-543 0162 - +31629 58 65 66
E-mailadres:	cindy.fatels@spaarnesant.nl

1) Is dit een vervolg op een eerdere melding?

Kies een van onderstaande opties.	Maak een keuze
a) Ja	
b) Nee	

2) Van wanneer dateert de oorspronkelijke melding?

(Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord).	Invullen
Datum:	

3) Wat is de strekking van de vervolgmelding?

(Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord, kies een van de volgende opties).	Maak een keuze
a) Toevoegen of wijzigen van informatie betreffende de eerdere melding	
b) Intrekking van de eerdere melding.	

4) Wat is de reden van intrekking?

(Beantwoord deze vraag als u bij vraag 3 hebt gekozen voor optie b).	Invullen
De reden van intrekking is:	

5) Geef een samenvatting van het incident waarop de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

6) Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

	Vul de aantallen in
a) Minimaal: (vul aan)	
b) Maximaal: (vul aan)	

7) Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

8) Wanneer vond de inbreuk plaats?

Kies een van de volgende opties:	Maak een keuze en vul in
a) Op (datum)	
b) Tussen (begindatum periode en einddatum periode).	
c) Nog niet bekend	

Wanneer werd de inbreuk ontdekt?

Op (datum)	

9) Wat is de aard van de inbreuk?

Reden	U kunt meerdere mogelijkheden kiezen
a) Lezen (vertrouwelijkheid)	Ja/nee
b) Kopiëren	Ja/nee
c) Veranderingen (integriteit)	Ja/nee
d) Verwijderen of vernietigen (beschikbaarheid)	Ja/nee
e) Diefstal	Ja/nee
f) Nog niet bekend	Ja/nee

10) Om welk type persoonsgegevens gaat het? U kunt meerdere mogelijkheden aankruisen.

Type persoonsgegevens	U kunt meerdere mogelijkheden kiezen.
a) Naam-, adres- en woonplaatsgegevens	Ja/nee
b) Telefoonnummers	Ja/nee
c) E-mailadressen of andere adressen voor elektronische communicatie	Ja/nee
d) Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam / wachtwoord of klantnummer)	Ja/nee
e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)	Ja/nee
f) Burgerservicenummer (BSN) of sofinummer	Ja/nee
g) Paspoortkopieën of kopieën van andere legitimatiebewijzen	Ja/nee
h) Geslacht, geboortedatum en/of leeftijd	Ja/nee
i) Bijzondere persoonsgegevens (Bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens).	Ja/nee. Zo ja welke
j) Overige gegevens, namelijk (vul aan)	

11) Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkene?

Gevolgen	U kunt meerdere mogelijkheden kiezen.
a) Stigmatisering of uitsluiting	Ja/nee
b) Schade aan de gezondheid	Ja/nee
c) Blootstelling aan (identiteits-) fraude	Ja/nee
d) Blootstelling aan spam of phishing	Ja/nee
e) Anders, namelijk (vul aan).	Ja/nee

12) Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

13) Wanneer is het datalek gemeld aan de Verwerkingsverantwoordelijke?

	Invullen

Datum en tijdstip:	
Contactpersoon Verwerkingsverantwoordelijke:	
Mededeling is gedaan per:	Maak keuze:
a) Telefoon	
b) E-mail	
c) Formulier	
d) Anders, namelijk	

14) Zijn de persoonsgegevens, versleuteld, gehasht[4] of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

	Kies een van de opties en vul waar nodig aan.
a) Ja	
b) Nee	
c) Deels, namelijk (vul aan):	

15) Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?
(Beantwoord deze vraag als u bij vraag 14 gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe).

16) Is naar uw mening deze melding compleet?

Selecteer een van de onderstaande opties.	Maak uw keuze
a) Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig.	
b) Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk.	

[4] Een gehasht wachtwoord betreft een opgeslagen versie van een wachtwoord dat niet te herleiden is tot het oorspronkelijke wachtwoord: er wordt namelijk gebruik gemaakt van een onomkeerbaar algoritme. Daardoor kan uit het wachtwoord wel de gehasthe vorm worden berekend (en worden gecontroleerd), maar uit de gehashte vorm niet het wachtwoord (en worden herleid).

Afsluitend:

Naam ondertekenaar Verwerker:	
Plaats:	
Datum:	
Handtekening:	

FORMULIER MET SPOED BESCHIKBAAR STELLEN AAN:
Contactpersoon bij Opdrachtgever:

Naam:	
Functie:	
Mobiele telefoon:	
E-mail:	

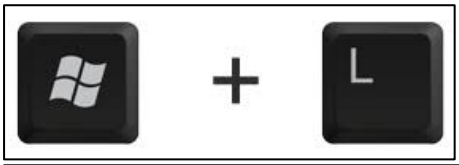
Het formulier is door Opdrachtgever ontvangen op:

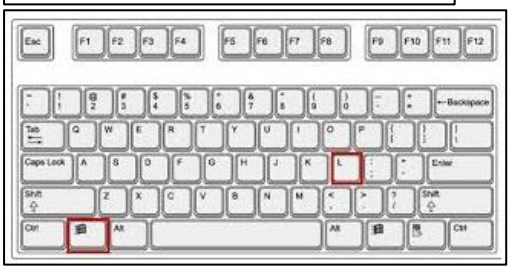
Datum en tijdstip:	

9. Bijlage CHECKLIST voor een AVG-PROOF werkplek!!!

Volg onderstaande instructie op zodat jouw werkplek AVG–PROOF is.

1. Als je je werkplek verlaat vergrendel je je werkstation door middel van het tegelijk indrukken van de “windows-toets” en “L”.





Je werkstation activeer je weer door op de spatiebalk te drukken en je wachtwoord in te vullen.

2. Zorg dat er geen persoonsgevoelige papieren op je bureau liggen als je de kamer verlaat.

3. Sluit kasten en je ladeblok af als je:
   a. voor langere tijd je werkplek verlaat (vergadering / lunch / afspraak buiten de deur) of
   b. als je naar huis gaat.

4. Zorg dat je papierbak leeg is als je naar huis gaat. Leeg je papierbak altijd in de afgesloten papiercontainer.
   Beter is papier direct in de afgesloten container te gooien.

5. Zorg dat er geen papieren op je bureau liggen als je naar huis gaat. Berg alles op in een kast/ladeblok en sluit deze af.

6. Printen doe je alleen indien dit echt nodig is en op elke printer heb je een beveiligingscode ingesteld.

10. Bijlage Beveiligd afdrukken instellen voor printer.

Je kunt beveiligd afdrukken op 2 manieren instellen, t.w.:

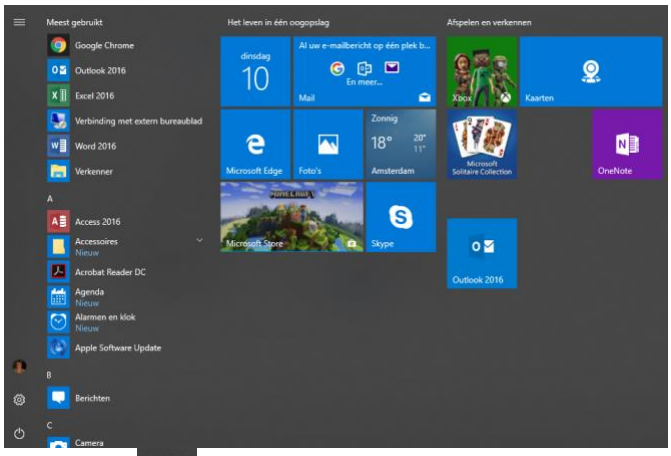
1. standaard instellen dat je via beveiligd afdrukken wilt werken of
2. per afdruk bepalen dat je via beveiligd afdrukken wilt werken.

Ad 1: Standaard instellen

Ga in Instellingen:

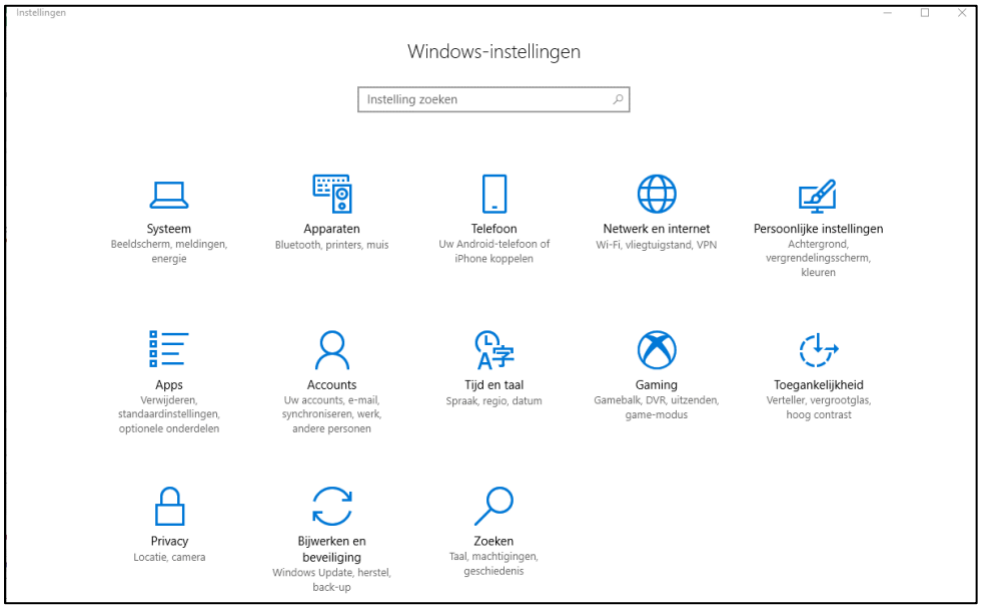
Klik op  links onderin je scherm.

Je ziet:

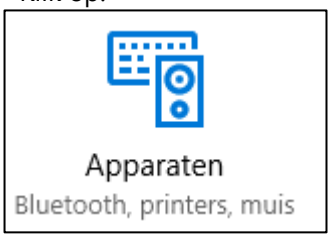


Klik op het  links onder je foto.

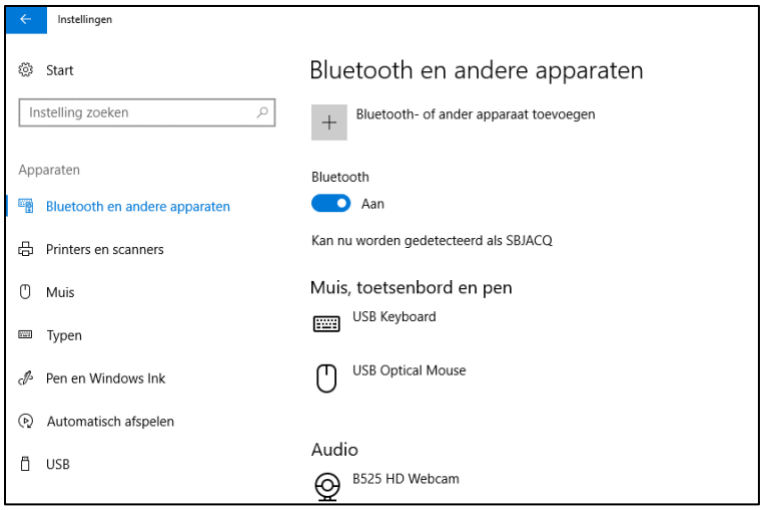
Je ziet dan:



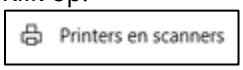
Klik op:



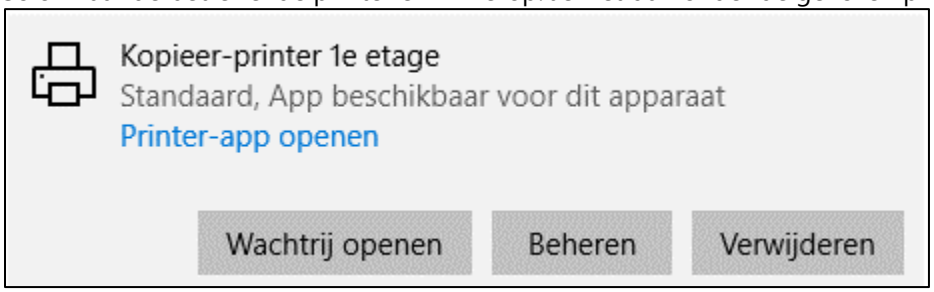
Je ziet dan:



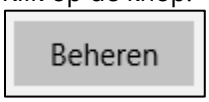
Klik op:



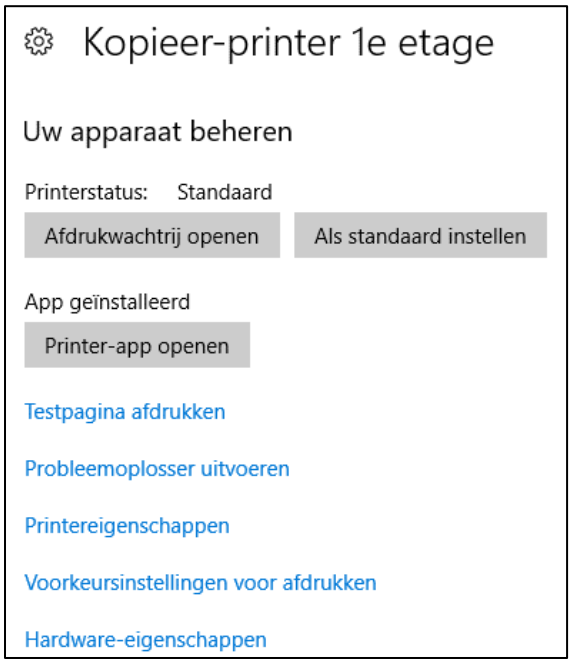
Scroll naar de betreffende printer en klik erop. Je ziet dan onder de gekozen printer opties verschijnen:



Klik op de knop:

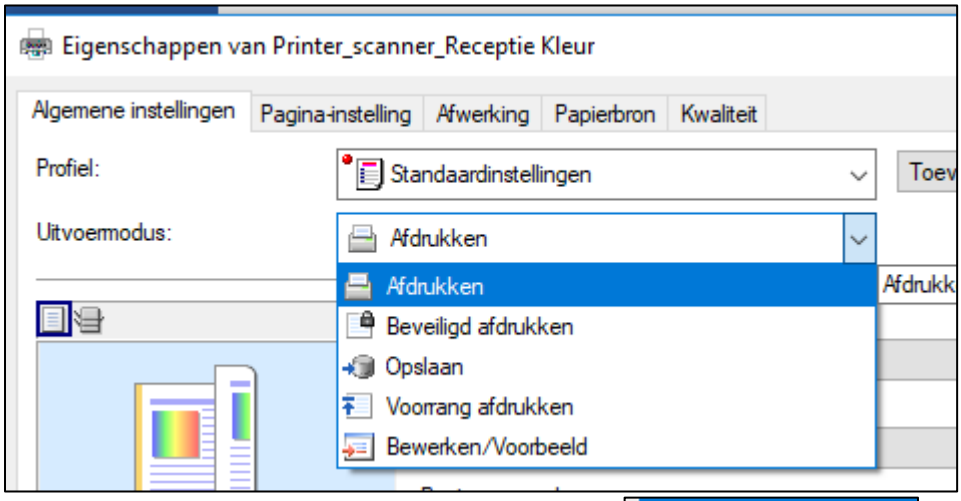


Je ziet:



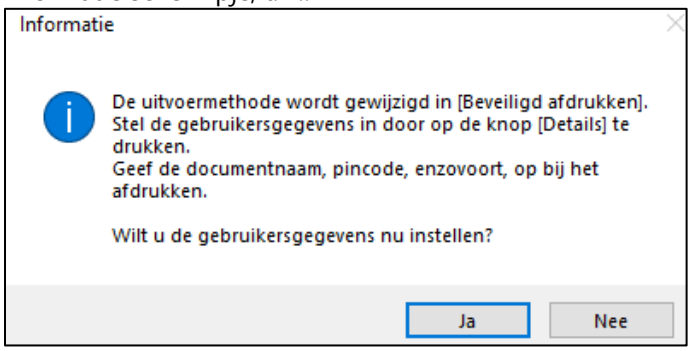
Klik op:

Je komt dan in onderstaand scherm:

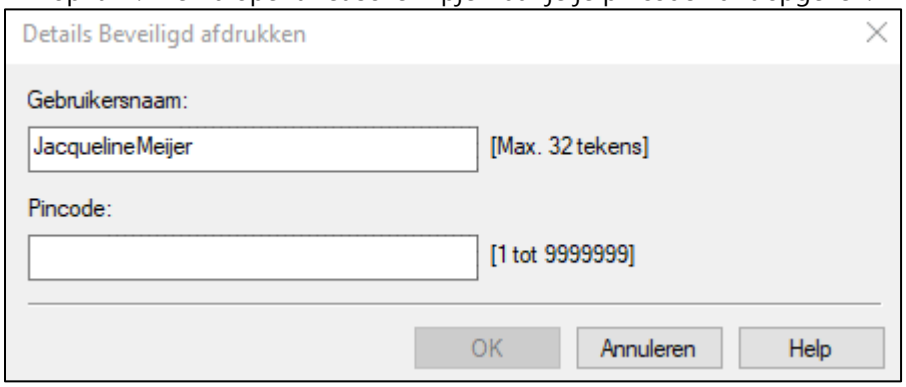


Klap achter Uitvoermodus het menu uit en kies voor 

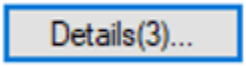
. Er verschijnt direct een informatie schermpje, t.w.:

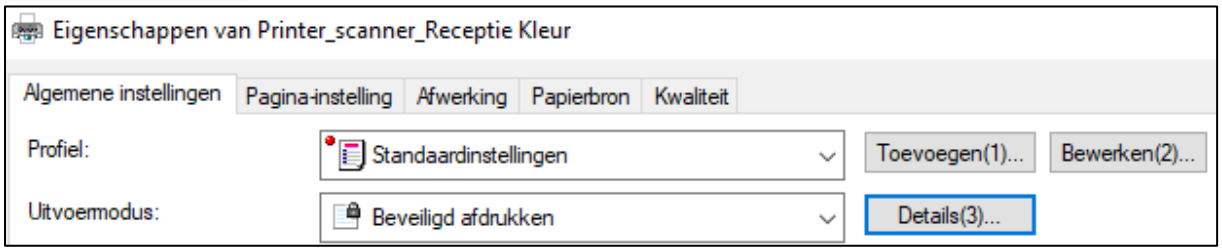


Klik op "JA". Hierna opent het schermpje waar je je pincode kunt opgeven.



Geef een pincode op en klik op "OK".
Je ziet nu achter de uitvoermodus de omschrijving beveiligd afdrukken en daar weer achter de knop





Klik je op deze knop dan kun je je pincode wijzigen.

LET OP: je moet dit per printer die je gebruikt instellen!!!!

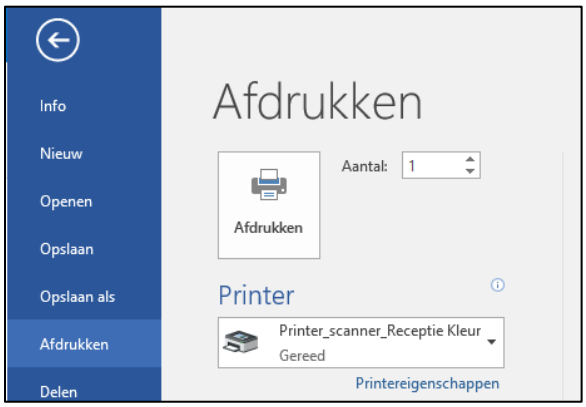
Ga nu naar de printer om je beveiligde print op te halen.

Ad 2: Per document bepalen.

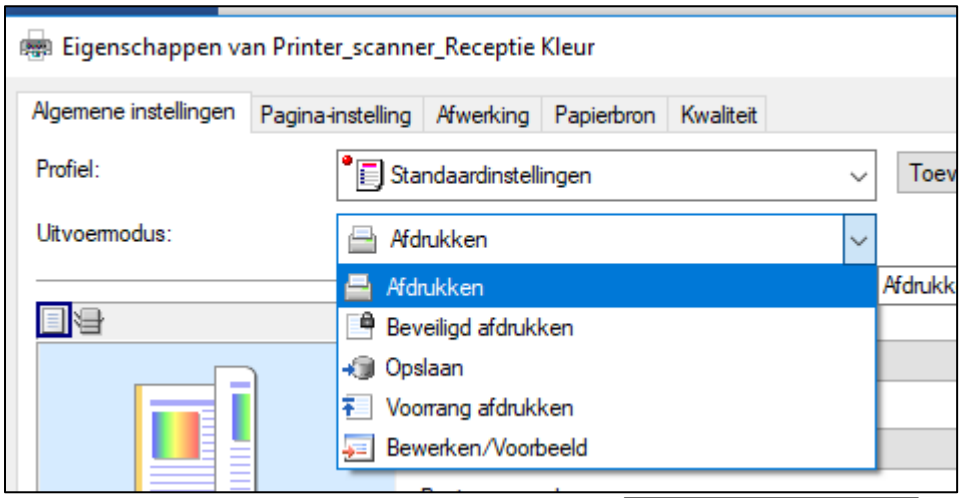
Ga in Word of Excel naar Afdrukken.

Dit doe je door op "Bestand" (links boven in je scherm Bestand) en dan op "Afdrukken" (6e optie van boven Afdrukken) te klikken. Of door middel van de toetscombinatie CTRL + P.

Je komt dan in onderstaand scherm en klik onder Printer op Printereigenschappen.

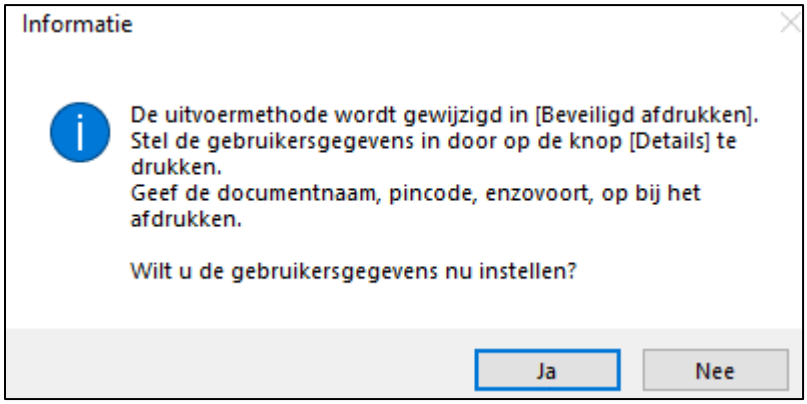


Je komt dan in onderstaand scherm:

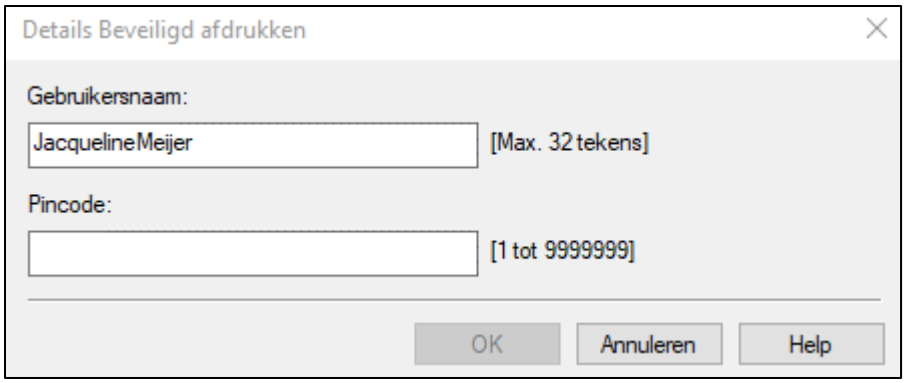


Klap achter Uitvoermodus het menu uit en kies voor 

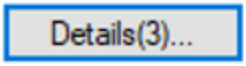
Er verschijnt direct een informatie schermpje, t.w.:

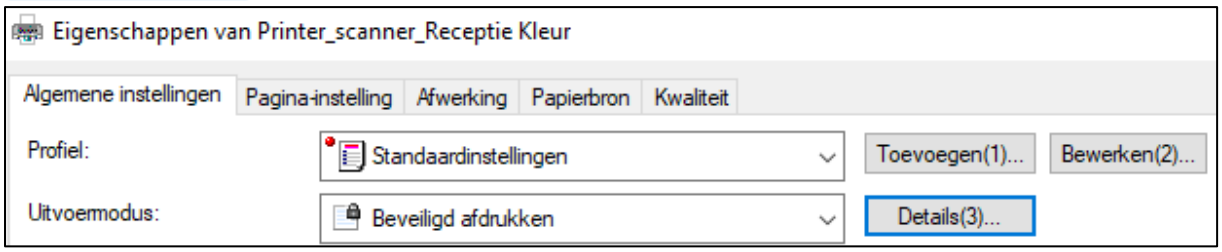


Klik op "JA". Hierna opent het schermpje waar je je pincode kunt opgeven.



Geef een pincode op en klik op "OK".
Je ziet nu achter de uitvoermodus de omschrijving beveiligd afdrukken en daar weer achter de knop





Klik je op deze knop dan kun je je pincode wijzigen.

LET OP: je moet dit per printer die je gebruikt instellen!!!!

Ga nu naar de printer om je beveiligde print op te halen.