



**Informatiebeveiligings- en privacy beleid**

**Haagsche Schoolvereniging**

<b>1</b>	<b>INLEIDING .....</b>	<b>3</b>
1.1	INFORMATIEBEVEILIGING EN PRIVACY .....	3
<b>2</b>	<b>DOEL EN REIKWIJDTE .....</b>	<b>3</b>
<b>3</b>	<b>UITGANGSPUNTEN .....</b>	<b>4</b>
3.1	ALGEMENE BELEIDSUITGANGSPUNTEN .....	
3.2	BELEIDSUITGANGSPUNTEN PRIVACY .....	4
<b>4</b>	<b>WET- EN REGELGEVING.....</b>	<b>5</b>
<b>5</b>	<b>ORGANISATIE .....</b>	<b>6</b>
5.1.1	RICHTINGGEVEND .....	6
5.1.2	STUREND.....	6
5.1.3	UITVOEREND.....	6
<b>6</b>	<b>CONTROLE EN RAPPORTAGE.....</b>	<b>6</b>
6.1	VOORLICHTING EN BEWUSTZIJN .....	6
6.2	CLASSIFICATIE EN RISICOANALYSE .....	7
6.3	INCIDENTEN EN DATALEKKEN .....	7
6.4	CONTROLE, NALEVING EN SANCTIES .....	7

## 1 Inleiding

Informatie en ict zijn noodzakelijk in de ondersteuning van het onderwijs. Omdat we met persoonsgegevens (van onszelf, leerlingen en anderen) werken, is privacywetgeving daarop van toepassing.

De informatie en ict van de HSV worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan worden bedreigd door een aanval, een vergissing, de natuur (bijv. overstroming of brand), etcetera. Het niet beschikbaar zijn van ict, incorrecte administraties en het uitlekken van gegevens kan leiden tot inbreuken op het geven van onderwijs en het vertrouwen in onze school.

Deze bedreigingen maken het noodzakelijk om maatregelen te treffen om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Het is noodzakelijk dat we duidelijk maken waar het om gaat, een doel stellen en de manier beschrijven waarop we dit doel willen bereiken.

### 1.1.1 Informatiebeveiliging en privacy

Informatiebeveiliging is een proces voor het beschermen van de HSV tegen risico's en bedreigingen met betrekking tot informatie en ict. Het richt zich op drie aspecten:

- Beschikbaarheid; informatie en aanverwante bedrijfsmiddelen zijn toegankelijk wanneer nodig;
- Integriteit; informatie en verwerkingsmethoden bevatten zo min mogelijk fouten;
- Vertrouwelijkheid; informatie is alleen toegankelijk voor diegenen die daartoe bevoegd zijn.

Privacy gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving. Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan. Vooral het aspect vertrouwelijkheid is hiervoor van belang. Informatiebeveiliging is daarom integraal onderdeel van privacy.

Om privacy goed te regelen is informatiebeveiliging nodig. Daarom zien we het als één onderwerp: informatiebeveiliging en privacy (IBP).

## 2 Doel en reikwijdte

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.

Dit beleid is een leidraad voor iedereen die betrokken is bij IBP binnen de HSV. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen in de HSV. Het is van toepassing op de hele organisatie waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.

Het informatiebeveiligings- en privacybeleid heeft raakvlak met andere beleidsgebieden, te weten:

- Algemeen veiligheids- en beveiligingsbeleid; met als aandachtsgebieden bedrijfshulpverlening, fysieke toegang en –beveiliging, crisismanagement, huisvesting en ongevallen;
- IT-beleid; met als aandachtsgebieden de aanschaf en het beheer van ict;
- Personeels- en organisatiebeleid; met als aandachtsgebieden in- en uitstroom van medewerkers, functiescheiding en vertrouwensfuncties;

Dit document maakt duidelijk waar de verantwoordelijkheden rondom informatiebeveiliging en privacy zijn belegd.

### 3 Uitgangspunten

De belangrijkste beleidsuitgangspunten bij de HSV zijn:

- Informatiebeveiliging en privacy dient te voldoen aan alle relevante wet- en regelgeving
- Veilig en betrouwbaar omgaan met informatie is de verantwoordelijkheid van iedereen
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich ‘fatsoenlijk’ gedragen met een eigen verantwoordelijkheid
- De HSV is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt
- De HSV maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy
- IBP is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is
- Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen
- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid

#### 3.1.1 Privacy

De HSV hanteert de vijf vuistregels voor privacy:

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 wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag:** verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie:** bij de verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. 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 deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast 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.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van toestemming, zal de HSV aan de betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

## 4 Wet- en regelgeving

De HSV voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 2.0' leidend bij het maken van afspraken met leveranciers.

## 5 Organisatie

Dit hoofdstuk beschrijft hoe IBP in de HSV is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau worden rollen, taken en verantwoordelijkheden beschreven.

Richtinggevend

### **Eindverantwoordelijke**

De bestuurder is eindverantwoordelijk voor IBP en stelt het beleid en de maatregelen vast op het gebied van informatiebeveiliging en privacy. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd. Binnen de scholen is de directeur verantwoordelijk voor het IBP (manager IBP).

#### 5.1.1 Sturend

### **Manager IBP**

Manager IBP is een rol op sturend niveau. Deze geeft terugkoppeling en advies geeft aan de eindverantwoordelijke en stuurt mensen aan. De manager IBP moet:

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

### **Functionaris voor Gegevensbescherming**

De functionaris voor gegevensbescherming (FG) houdt binnen de HSV toezicht op de toepassing en naleving van de privacy-wetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. De FG is meestal ook contactpersoon en voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.

#### **5.1.2 In de praktijk**

##### **Medewerker**

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in het personeelshandboek. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers wordt 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 GMR)

##### **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 medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het IBP-beleid door 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 functionaris voor de gegevensbescherming.

## **6 Controle en rapportage**

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld. Hierbij wordt rekening gehouden met:

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

### **6.1.1 Voorlichting en bewustzijn**

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij

de HSV het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP en de bestuurder als eindverantwoordelijke.

#### **6.1.2 Classificatie en risicoanalyse**

Bij de HSV heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de 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 kwaliteitsaspecten die van belang voor de informatievoorziening.

#### **6.1.3 Incidenten en datalekken**

Alle incidenten kunnen worden gemeld bij de functionaris voor gegevensbescherming. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

#### **6.1.4 Controle, naleving en sancties**

Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de bestuurder, en heeft een wettelijk omschreven en onafhankelijke toezichhoudende taak. Mocht de naleving ernstig tekort schieten, dan kan de HSV de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden. Bij de HSV is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.