Informatiebeveiligings- en privacy beleid

Stichting Vrijescholen Zuidwest Nederland

De Vrije School Den Haag, basisschool

Bron:
saMBO-ICT
Kennisnet

Bewerkt door:
De Vrije School Den Haag , N.E. Schieman

Vastgesteld door Stichting Vrijescholen Zuidwest Nederland

Versie	Datum	Naam	Functie
		Artho Jansen	Bestuurder

1 Inleiding

Informatie en ICT zijn noodzakelijk in de ondersteuning van het onderwijs. De school werkt met persoonsgegevens (van onszelf, leerlingen en anderen) waarop de huidige privacywetgeving van toepassing is.

De informatie en ICT van De Vrije School Den Haag kunnen worden blootgesteld aan bedreigingen, bijvoorbeeld een aanval, een vergissing, de natuur (bijv. overstroming of brand) etc. Het niet beschikbaar zijn van ICT, een incorrecte administratie en het uitlekken van gegevens leidt tot inbreuken op het geven van onderwijs en het vertrouwen in de school.

Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Om dit structureel op te pakken is het noodzakelijk een informatie- en veiligheidsbeleid te hanteren.

1.1.1 Informatiebeveiliging en privacy

Informatiebeveiliging beschermt De Vrije School Den Haag 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 betreft de bescherming van persoonsgegevens conform de huidige wet- en regelgeving. Vooral het aspect vertrouwelijkheid is hiervoor van belang. Informatiebeveiliging is daarom integraal onderdeel van privacy. Om die reden ziet de school informatiebeveiliging en privacy (IBP) als één onderwerp.

2 Doel en reikwijdte

Dit beleid heeft tot doel:

- 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 Vrije School Den Haag. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen in De Vrije School Den Haag. Het is van toepassing op de hele organisatie van De Vrije School Den Haag, waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.

Het informatiebeveiligings- en privacy-beleid 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 beleid maakt duidelijk waar de verantwoordelijkheden rondom informatiebeveiliging en privacy zijn belegd.

3 Uitgangspunten

De belangrijkste beleidsuitgangspunten bij De Vrije School Den Haag zijn:

- Informatiebeveiliging en het 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 zorgvuldig omgaan met privacy gevoelige informatie waar zijn verantwoordelijk voor zijn.
- De Vrije School Den Haag is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.
- De Vrije School Den Haag maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy.
- IBP is een continu proces. Een evaluatie vindt minimaal jaarlijks plaats, waarbij gekeken wordt of aanpassing gewenst is.
- Er is een juiste balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- Er is een juiste balans tussen privacy, functionaliteit/werkbaarheid en veiligheid.

3.1.1 Privacy

De Vrije School Den Haag hanteert de volgende 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; de gegevens staan in verhouding tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer worden bewaard dan noodzakelijk. De school hanteert de wettelijke bewaartermijnen.
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. Betrokkenen kunnen 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 Vrije School Den Haag aan de betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

4 Wet- en regelgeving

De Vrije School Den Haag voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens tot 1 mei 2018
- Algemene Verordening Gegevensbescherming (AVG) na 1 mei 2018
- 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 Vrije School Den Haag is georganiseerd. Er wordt daarbij onderscheid gemaakt op drie niveaus:

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

Bij elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

5.1.1 Richtinggevend

Eindverantwoordelijke
Het bestuur 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 door het bestuur geëvalueerd. Binnen de school is de schoolleider verantwoordelijk voor IBP.

5.1.2 Sturend

Manager IBP (Niels Schieman)
Manager IBP is een rol op sturend niveau. Deze geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen in de uitvoerende laag aan. De manager IBP moet:

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

Functionaris voor Gegevensbescherming (Anna Italianer)
De functionaris voor gegevensbescherming (FG) houdt binnen De Vrije School Den Haag toezicht op de toepassing en naleving van de privacywetgeving. 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. FG heeft regelmatig overleg met manager IBP. De FG is meestal ook contactpersoon voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.

Domeinverantwoordelijkheid/proceseigenaar
Binnen de school zijn er verschillende domeinen/processen, zoals ICT, personeel, administratie et cetera. Elk domein en proces heeft een eigen verantwoordelijke om te bepalen op welke wijze IBP wordt vormgegeven in richtlijnen, procedures en instructies.

Leidinggevenden hebben een voorbeeldrol ten opzichte van hun medewerkers.

5.1.3 Uitvoerend

Security Officer (Ralph van den Heuvel)
De Security Officer vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging.

Functioneel beheerder
Op basis van de domeinverantwoordelijke/proceseigenaar heeft de functioneel beheerder een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Medewerker
Alle medewerkers hebben een eigen verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in het personeelshandboek en de handleiding ‘aanvaardbaar gebruik van bedrijfsmiddelen’. 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:

- Ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid.
- 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 manager IBP.

6 Controle en rapportage

Dit informatiebeveiligings- en privacy-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door de functionaris gegevensbescherming. De bestuurder en de schoolleider worden hierover geïnformeerd . 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.

Daarnaast kent De Vrije School Den Haag een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacy-beleid wordt getoetst.

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 Vrije School Den Haag het bewustzijn van de individuele medewerkers 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, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP met het bestuur als eindverantwoordelijke.

6.1.2 Classificatie en risicoanalyse

Bij De Vrije School Den Haag 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.

Incidenten en datalekken
Alle incidenten kunnen worden gemeld bij de functionaris gegevensbescherming (FG). De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Melding van datalekken is mogelijk via https://autoriteitpersoonsgegevens.nl/

6.1.3 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij De Vrije School Den Haag wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Met betrekking tot de bevordering van de naleving van de Wet Bescherming Persoonsgegevens vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het bestuur, en heeft een wettelijk omschreven, onafhankelijke toezichthoudende taak.
Mocht de naleving ernstig tekort schieten, dan kan De Vrije School Den Haag de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
Bij De Vrije School Den Haag wordt de handelswijze met betrekking tot het melden van beveiligingsincidenten en datalekken vastgelegd in een privacyreglement en/of protocol.

Bijlage 1: Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Voorbeelden: Bestuur CvB Directeur	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	Manager IBP	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Bewerkersovereenkomsten regelen • Brief toestemming gebruik foto's en video • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ICT en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming / Privacy officer	• Toezicht op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement. • Procedure IBP-incident afhandeling. • Inrichten meldpunt datalekken.
	Domeinverantwoordelijke/ Proceseigenaren waaronder: ICT, personeel (HRM / P&O), Facilitair, onderwijs, financien, inkoop en administratie	• **Classificatie / risicoanalyse** *in samenwerking met Manager IBP (Informatiemanager / verantwoordelijke IBP / Security officer)* • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door *bestuur/CvB/directie* • *Samen met functioneel beheer en ICT beheer* er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • *Samen met functioneel beheer en ICT* beheer de toegangsrechten van gebruikers regelmatig beoordelen en	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst). • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk.

		controleren.	

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen Vanuit de Wiki
Uitvoerend (operationeel)	Security officer	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten.	
	Functioneel beheerder	• Uitvoeren taken conform gegeven richtlijnen en procedures.	
	Medewerker	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	Communiceren, informeren en toezien op naleving van o.a.:
	Dagelijkse leiding / leidinggevende / directie	• Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	• IBP in het algemeen. • Regels passend onderwijs . • Hoe omgaan met leerling dossiers. • Wie mogen wat zien. • Gedragscode. • Omgaan met sociale media. • Mediawijs maken.