Informatiebeveiliging en privacy De Nieuwe Veste

Inhoudsopgave

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 Nieuwe Veste 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. Het niet beschikbaar zijn van ICT, incorrecte administraties en het uitlekken van gegevens tot inbreuken op het geven van onderwijs en het vertrouwen in onze 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 dat we een duidelijk maken waar het om gaat, een doel stellen en de manier waarop we dit doel willen bereiken.

Informatiebeveiliging
Informatiebeveiliging is een proces voor het beschermen van De Nieuwe Veste tegen risico's en bedreigingen met betrekking tot informatie en ICT. Het is een samenhangend geheel van preventieve, repressieve en herstelmaatregelen alsmede procedures en processen welke de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen blijvend garanderen met als doel de continuïteit van de bedrijfsvoering te waarborgen en eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald, niveau te beperken.

Informatiebeveiliging omvat een *samenhangend stelsel* van maatregelen. Dit betekent dat de verschillende maatregelen die samen de informatiebeveiliging vormen niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan.

Zoals in de voorgaande definitie is verwoord, richt informatiebeveiliging zich op de volgende drie aspecten van de informatievoorziening:
- *Beschikbaarheid:* het waarborgen dat geautoriseerde gebruikers, entiteiten of processen toegang hebben tot informatie en de informatiesystemen op de gewenste momenten.
- *Integriteit;* het waarborgen dat de informatie juist en volledig is en de informatiesystemen juiste en volledige informatie opslaan en verwerken.
- *Vertrouwelijkheid*: het waarborgen dat informatie alleen toegankelijk is voor personen, entiteiten of processen die hiertoe bevoegd / geautoriseerd zijn.

Het stelsel van beveiligingsmaatregelen heeft tot doel een *blijvend niveau van beveiliging* te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn blijft gehandhaafd.

Informatiebeveiliging is gericht op het realiseren van een *optimaal niveau van beveiliging.* Dit optimum wordt bereikt door een zorgvuldige afweging van kosten en baten.

Privacy
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 (hierna: IBP).

2. Doel en reikwijdte

Het opstellen van het beleid IBP binnen De Nieuwe Veste heeft tot doel:
- het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering;
- het garanderen van de privacy van leerlingen, hun ouders en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen;
- de uitgangspunten met betrekking tot IBP binnen de school vast te leggen en formeel vast te stellen.

Het beleid IBP is een leidraad voor alle betrokkenen binnen De Nieuwe Veste. Het beleid is expliciet van toepassing op de leerlingen, hun ouders/verzorgers[1], de leden van de Raad van Toezicht (hierna: RvT) en alle medewerkers van De Nieuwe Veste en (andere) personen die in opdracht van de school werkzaam zijn zoals, stagiaires, vrijwilligers, gedetacheerden en uitzendkrachten. Het beleid is toepassing op de hele organisatie, waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden. Het beleid maakt duidelijk waar de verantwoordelijkheden rondom IBP zijn belegd.

Het beleid IBP heeft raakvlak met andere beleidsgebieden, te weten:
- algemeen veiligheids- en beveiligingsbeleid; met als aandachtsgebieden bedrijfshulpverlening, fysieke toegang en –beveiliging, crisismanagement, huisvesting en ongevallen;
- ICT-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.

3. Uitgangspunten

De belangrijkste beleidsuitgangspunten bij De Nieuwe Veste zijn:
- IBP dient te voldoen aan alle relevante wet- en regelgeving en doet recht aan het open karakter van de school;
- IBP betreft de primaire processen en de bedrijfsvoering is open waar het kan en gesloten waar het moet;
- veilig en betrouwbaar omgaan met informatie is de verantwoordelijkheid van iedereen, waarbij vertouwen de basis is;
- IBP is een vanzelfsprekend en integraal onderdeel van de school (lijnverantwoordelijkheid);
- er wordt van alle medewerkers, leerlingen, hun ouders, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich ‘fatsoenlijk’ gedragen met een eigen verantwoordelijkheid;
- om te borgen dat personen de continuïteit van de school niet in gevaar brengen zijn processen, procedures, richtlijnen en gedragscodes geformuleerd en geïmplementeerd;
- bij overtreding kan het College van Bestuur een sanctie opleggen;
- De Nieuwe Veste is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt en is daarmee verantwoordelijk voor de beveiliging ervan;
- De Nieuwe Veste maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over IBP;
- IBP is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is;

[1] Waar in deze beleidsnotitie staat ouders worden ook verzorgers bedoeld.

- afwijkingen van en wijzigingen op het beleid worden beargumenteerd en gebeuren op basis van risico-analyses;
- bij (ICT) projecten betreffende primaire processen en bedrijfsvoering wordt vanaf de start rekening gehouden met IBP;
- 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.

De Nieuwe Veste 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 Nieuwe Veste aan de betrokkenen een eenduidige zogenaamde Opt-out procedure worden aangeboden. Dit houdt in, dat betrokkenen kunnen afzien van het geven van toestemming.

4. Wet- en regelgeving

Voor IBP-beleid is wet- en regelgeving van toepassing. De Nieuwe Veste voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- wet op het voortgezet onderwijs;
- wet goed onderwijs en goed bestuur VO;
- wet bescherming persoonsgegevens; / algemene Verordening Gegevensbescherming (AVG);
- archiefwet;
- leerplichtwet;
- auteurswet;
- wetboek van Strafrecht.

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

Daarnaast zijn een privacyreglement en interne richtlijnen en gedragscodes opgesteld voor iedereen die werkt of leert bij De Nieuwe Veste of gebruik maakt van de informatievoorzieningen van de school. Deze zijn te vinden in map 108 van het personeelshandboek en op de website van de school.

5. Organisatie

Dit hoofdstuk beschrijft hoe IBP in De Nieuwe Veste is georganiseerd. Er wordt beschreven welke rollen, welke taken en verantwoordelijkheden hebben.

College van Bestuur
Het College van Bestuur (hierna: CvB) 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 CvB geëvalueerd. De directeur bedrijfsvoering is verantwoordelijk voor informatiebeveiliging.

Functionaris gegevensbescherming en gegevensverwerking
De functionaris gegevensbescherming en gegevensverwerking (hierna: FG) geeft terugkoppeling en advies aan het CvB, vertaalt het beleid IBP naar richtlijnen, procedures, maatregelen en documenten en bewaakt de uniformiteit binnen de school. De FG houdt binnen De Nieuwe Veste 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 is aanspreekpunt voor (incidenten) op het gebied van IBP en zorgt (mede) voor het coördinateren/afhandelen van (vertrouwelijke) informatiebeveiligingsincidenten. FG heeft regelmatig overleg met het CvB over IBP en met de directeur bedrijfsvoering en het hoofd ICT over informatiebeveiliging. Voor meer informatie verwijzen we naar de taakomschrijving FG.

Directieleden / leidinggevenden
De naleving van het beleid IBP is onderdeel van de integrale bedrijfsvoering. Ieder(e) directielid, leidinggevende heeft de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beleid IBP en de bijbehorende richtlijnen, procedures, maatregelen en documenten;
- toe te zien op de naleving van het beleid IBP door de medewerkers, waarbij hij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in bijvoorbeeld werkoverleggen, de gesprekkencyclus.
- als aanspreekpunt beschikbaar te zijn voor alle medewerkers gerelateerde IBP onderwerpen.

Hoofd ICT
Het hoofd ICT vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging.

Medewerkers
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden en binnen de eigen invloedssfeer. De medewerkers worden geacht op de hoogte zijn van en zich te houden aan het beleid IBP en de bijbehorende richtlijnen, procedures, maatregelen en documenten.
De medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).

Leerlingen
Alle leerlingen hebben verantwoordelijkheid met betrekking tot informatiebeveiliging binnen de eigen

invloedssfeer, zoals het zich houden aan de richtlijnen en procedures van de school op het gebied van IBP. De leerlingen worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van incidenten.

Incident Response Team
De Nieuwe Veste beschikt over een Incident Response Team (hierna: IRT) voor het coördinateren/afhandelen van (vertrouwelijke) informatiebeveiligingsincidenten. Het IRT bestaat uit de volgende vaste leden:
- de voorzitter CvB;
- de FG;
- het hoofd ICT.

Zo nodig wordt het IRT – na een afweging daartoe van de voorzitter CvB - aangevuld met:
- een forensisch IT-deskundige;
- een juridisch adviseur; en/of
- een communicatieadviseur.

Voor meer informatie over de (werkwijze) van het IRT verwijzen wij naar het handboek datalekken De Nieuwe Veste.

6. Controle en rapportage

De school kent een jaarlijkse planning en control cyclus voor IBP. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het beleid IBP wordt getoetst.

Het beleid IBP wordt minimaal elke twee jaar getoetst en bijgesteld door de directie. 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.

Voorlichting en bewustzijn
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van IBP uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij De Nieuwe Veste het bewustzijn van de individuele medewerkers, leerlingen en hun ouders voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingscampagnes.

Classificatie en risicoanalyse
Bij De Nieuwe Veste 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 risico-analyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang voor de informatievoorziening.

Incidenten en datalekken
Indien een medewerker een (mogelijke) inbreuk op de beveiliging signaleert waarbij (mogelijk) persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, meldt de medewerker dit per omgaande aan de FG ongeacht het tijdstip van de dag.
De FG meldt vervolgens op zijn beurt per omgaande de (mogelijke) inbreuk op de beveiliging telefonisch aan de voorzitter van het CvB en het hoofd van de ICT-afdeling en bevestigt dit hen per

e-mail, tenzij er gegronde redenen zijn om de (mogelijke) inbreuk niet per e-mail te bevestigen (bijvoorbeeld indien daarmee duidelijk zou (kunnen) worden voor hackers dat hun hack is ontdekt). Iedere medewerker is te allen tijde bevoegd zelfstandig een melding te doen bij de voorzitter van het CvB (telefoonnummer/e-mailadres), dus ook bij het ontbreken van een voorafgaande melding aan de FG.
Door middel van de melding aan de FG en/of de voorzitter van het CvB wordt de procedure als verwoord in het handboek datalekken De Nieuwe Veste daadwerkelijk gestart.

CyberEdge verzekering
De school heeft een CyberEdge verzekering afgesloten. Als onderdeel van deze verzekering kunnen we een beroep doen op gespecialiseerde consultants die ons bijstand bieden tijdens een vermeend cyberincident. De specialisten zijn dag en nacht, 365 dagen per jaar beschikbaar voor strategisch en operationeel crisismanagement. Nadat de voorzitter van het CvB over een (mogelijk) datalek is geïnformeerd, wordt direct contact opgenomen met de AIG CyberEdge Hotline. Voor meer informatie verwijzen we naar handboek datalekken De Nieuwe Veste.

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 Nieuwe Veste wordt actief aandacht besteed aan IBP bijvoorbeeld bij de aanstelling, tijdens gesprekken in het kader van de gesprekkencyclus en met periodieke bewustwordingscampagnes.
Voor de bevordering van de naleving van de privacywet vervult de FG een belangrijke rol.
De FG wordt aangesteld door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.
Mocht de naleving ernstig tekort schieten, dan kan De Nieuwe Veste de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO-VO en de wettelijke mogelijkheden.

Bijlage 1: Tabel IBP rollen en taken

Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
CvB	• 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/taakomschrijving FG vaststellen • Privacyreglement vaststellen
FG	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert CvB over IBP • Voorbereiden uitvoeren IBP-beleid/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 • Toezicht op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • privacyreglement • handboek datalekken • gedragscode ICT gebruik waaronder sociale media • bewerkersovereenkomsten regelen • toestemming gebruik foto's en video • informatie documentatie richting medewerkers, leerlingen, ouders / verzorgers (bewustwording IBP)
Directie/ leidinggevende	• 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, gesprekkencyclus etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan CvB.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken

Directeur bedrijfsvoering	• Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door CvB • *Samen met hoofd ICT:* er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • *Samen met hoofd ICT;* beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• 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
Hoofd ICT	• *Samen met directeur bedrijfsvoering:* er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • *Samen met directeur bedrijfsvoering;* beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren. • Samen met FG/IRT Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten.	• Classificatie- en risicoanalyse documenten. • Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: toegangsmatrix diverse informatiesystemen en netwerk