Informatiebeveiligings- en privacybeleid

Christelijk College de Noordgouw

Ingangsdatum: 1 april 2021

AVG werkgroep

Christelijk College de Noordgouw

Inhoud

1.0 INLEIDING 3

1.1 INFORMATIEBEVEILIGING EN PRIVACY 3

2.0 DOEL EN REIKWIJDTE 3

3.0 UITGANGSPUNTEN 4

3.1 BELANGRIJKSTE BELEIDSUITGANGSPUNTEN 4
3.2 BELEIDSUITGANGSPUNTEN PRIVACY 4

4.0 WET- EN REGELGEVING 5

5.0 ORGANISATIE 5

5.1 RICHTINGGEVEND EN STUREND 5
5.2 UITVOEREND 5
5.3 FUNCTIONARIS VOOR GEGEVENSBESCHERMING 5
5.4 DOMEINVERANTWOORDELIJKHEID/PROCESEIGENAAR 5
5.5 MEDEWERKER 6
5.6 LEIDINGGEVENDE 6

6.0 CONTROLE EN RAPPORTAGE 6

6.1 VOORLICHTING EN BEWUSTZIJN 6
6.2 CLASSIFICATIE EN RISICOANALYSE 6
6.3 INCIDENTEN EN DATALEKKEN 7
6.4 CONTROLE, NALEVING EN SANCTIES 7

	datum	***voorlopige status***	***datum***	***definitieve status***
Directie	*11-02-2021*	*voorgenomen besluit*	*19-02-2021*	*vastgesteld*
MR	*18-02-2021*	*ter advisering*	*18-02-2021*	*positief advies*
RvB		*nvt*		
Geldig tot	*1 april 2023*			

1.0 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 school 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), et cetera. Het niet beschikbaar zijn van ict, incorrecte administraties en het uitlekken van gegevens leidt 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 duidelijk maken waar het om gaat, een doel stellen en de manier waarop we dit doel willen bereiken.

1.1 Informatiebeveiliging en privacy
Informatiebeveiliging is een proces voor het beschermen van de school 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 een integraal onderdeel van privacy.

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

2.0 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 school. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen in de school. Het is van toepassing op de hele organisatie, waaronder de fysieke locatie, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.

Het informatiebeveiligings- en privacybeleid heeft raakvlakken 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.

3.0 Uitgangspunten

3.1 Belangrijkste beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten zijn:

- Informatiebeveiliging en het privacybeleid dienen te voldoen aan alle relevante wet- en regelgeving.
- Veilig en betrouwbaar omgaan met informatie en 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 Stichting voor Christelijk Voortgezet Onderwijs te Heerde is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.
- De school 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.

3.2 Beleidsuitgangspunten privacy

Wij hanteren 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 persoonsgegeven 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 CC de Noordgouw aan de betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

4.0 Wet- en regelgeving

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

- Wet op het voortgezet 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 3.0' leidend bij het maken van afspraken met leveranciers.

5.0 Organisatie

5.1 Richtinggevend en sturend

De rector-bestuurder is eindverantwoordelijk voor IBP en stelt het beleid en de maatregelen vast op het gebied van informatiebeveiliging en privacy. De rector-bestuurder geeft tevens sturing aan de taken die bij de uitvoering van taken die bij IBP horen. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages door het bevoegd gezag (Raad van Beheer) en de MR geëvalueerd. Binnen de RvB is de rector-bestuurder verantwoordelijk voor IBP. Verder zijn de daarbij behorende taken:

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

5.2 Uitvoerend

Binnen de administratie is een medewerker belast met de administratieve ondersteuning van de rector-bestuurder om het IBP vorm te geven en up-to-date te houden. Daarnaast zullen de diverse (staf)medewerkers hen ondersteunen op het voor hun relevante werkveld.

5.3 Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt toezicht op de toepassing en naleving van de privacy-wetgeving. De wettelijke taken en bevoegdheden van de FG vereisen dat deze functionaris een onafhankelijke positie in de organisatie inneemt. De FG zorgt ook voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. Deze taak is buiten de school ondergebracht bij een externe functionaris (belegd bij de Lumengroup) die in ViA-verband is aangesteld. Hiermee is de onafhankelijkheid en de kwaliteit gewaarborgd.

5.4 Domeinverantwoordelijkheid/proceseigenaar

Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel, administratie et cetera. Op elk van deze domeinen/processen wordt iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Leidinggevenden hebben een voorbeeldrol ten opzichte van hun medewerkers.

5.5 Medewerker

Alle medewerkers hebben 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 onder andere gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door melding te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).

5.6 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 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 rector-bestuurder.

6.0 Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door de schoolleiding. 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 CC de Noordgouw een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

6.1 Voorlichting en bewustzijn

Het beleid formuleren en daarbij behorende maatregelen nemen 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 het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de rector-bestuurder als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse

Bij CC de Noordgouw 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.

6.3 Incidenten en datalekken

Alle incidenten moeten worden gemeld bij **datalek@noordgouw.nl**. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

6.4 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. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het bevoegd gezag, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het RvB vast te stellen reglement.
Mocht de naleving ernstig tekort schieten, dan kan CC de Noordgouw de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
Bij CC de Noordgouw is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.