NTC Firenze - Informatiebeveiliging en Privacy (IBP)

Documentgegevens

Versiebeheer

Versie	Datum versie	Wijzigingen
0.1	06-05-2018	Initiële versie, gebaseerd op de aanpak IBP voor het PO en VO van BRON en model documenten
0.2	31-12-2020	Verwijdering paragrafen die reeds doorgestreept waren; geen belofte van vermelding IBP beleid op website meer (website wordt niet bijgehouden); vermelding verantwoordelijkheid docenten voor data mbt onderwijs (1.5); update internet en social media.

Goedkeuring

Versie	Datum vastgesteld	Vastgesteld door
0.2	6 februari 2021	ALV

Distributie

Versie	Datum gedeeld	Gedeeld met
0.1	06-05-2018	Bestuur (Katrien, Ivo, Imco, Piet)
0.2	31-12-2020	Bestuur (Bianca, Lapo, Sarah), docenten en ALV

Inhoud

Inleiding

Scholen maken steeds beter en meer gebruik van ICT. Daardoor neemt niet alleen het aantal persoonsgegevens dat scholen gebruiken toe. Ook brengt de afhankelijkheid van ICT nieuwe risico's met zich mee, zoals cybercrime en datalekken. Het beschermen van de persoonsgegevens van leerlingen en docenten en daarmee het waarborgen van de privacy, wordt dan ook steeds belangrijker. Schoolbestuurders zijn volgens de wet verplicht om privacy goed te regelen.

Wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen genomen moeten worden om de persoonsgegevens te beschermen. Informatiebeveiliging is een belangrijke voorwaarde voor privacy, terwijl omgekeerd het zorgvuldig omgaan met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar en zijn van elkaar afhankelijk.

Om makkelijk over informatiebeveiliging en privacy te kunnen praten korten we het af tot IBP.

AVG

Vanaf 25 mei 2018 is er nog maar één privacywet voor de hele Europese Unie. De **Algemene verordening gegevensbescherming (AVG)**. Deze nieuwe wetgeving sluit aan op technologische ontwikkelingen en globalisering. Door de AVG zijn persoonsgegevens van alle EU-inwoners straks op dezelfde wijze beschermd, ongeacht of hun gegevens zijn opgeslagen in Europa of bijvoorbeeld de Verenigde Staten.

Dat betekent dat er vanaf 25 mei 2018 nog maar één privacywet geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. De AVG is een verordening, dit houdt in dat er rechtstreeks verplichtingen worden opgelegd aan organisaties die persoonsgegevens verwerken en rechten worden toegekend aan betrokkenen (degenen van wie persoonsgegevens verwerkt worden).

Als de AVG van toepassing is, hebben organisaties die persoonsgegevens verwerken meer verplichtingen. Er wordt in de AVG meer nadruk gelegd op de verantwoordelijkheid van organisaties (scholen) zelf. Scholen moeten niet alleen de wet naleven, zij moeten kunnen aantonen dat zij zich aan de wet houden.

De volgende tien onderwerpen laten niet alleen de uitbreidingen en aanpassingen van de huidige regels van de Wbp zien, maar bevatten ook de nieuwe elementen die zijn toegevoegd in de AVG.

1. Uitgangspunten privacy (5 vuistregels2.0)
2. Privacy by design / by default
3. Verplichte risicoanalyse
4. Documentatieplicht
5. Bewustzijn creëren en voorlichten
6. Gebruik digitale diensten onder de 16 jaar
7. Verwerkersovereenkomsten
8. Meldplicht datalekken
9. Functionaris voor gegevensbescherming
10. Technische en organisatorische maatregelen

1 Informatiebeveiliging en Privacy

(Dit hoofdstuk bevat de modeltekst voor IBP van Stichting Kennisnet).

1.1 Toelichting

1.1.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.

- Informatiebeveiliging richt zich op de volgende aspecten:
- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

1.1.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. 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.

1.1.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis op informatiebeveiliging en privacy binnen het NTC Firenze te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

1.2 Doel en reikwijdte

1.2.1 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 het NTC Firenze persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en docenten.
- 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. docenten, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en het NTC Firenze voldoet aan relevante wet- en regelgeving.

1.2.2 Reikwijdte

- Het IBP-beleid binnen het NTC Firenze geldt voor alle docenten, leerlingen, ouders/verzorgers.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen het NTC Firenze waaronder in ieder geval alle docenten, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan het NTC Firenze persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen die vallen onder de verantwoordelijkheid van het NTC Firenze. 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 docenten 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 het NTC Firenze 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.
- IBP-beleid heeft binnen het NTC Firenze raakvlakken met:
    - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van docenten, functiewisselingen, functiescheiding en vertrouwensfuncties
    - Medezeggenschap van leerlingen, hun ouders/verzorgers en docenten.

1.3 Beleid – Hoe doen we dat?

Het NTC Firenze hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van het NTC Firenze neemt de verantwoordelijkheid om 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.
2. Het NTC Firenze voldoet aan alle relevante wet- en regelgeving.
3. Bij het NTC Firenze 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 het NTC Firenze 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.

4. Het NTC Firenze zal alle betrokkenen helder en actief informeren over de verwerkingen van de 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 en profilering.
5. Het NTC Firenze legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Het NTC Firenze voldoet hiermee aan de documentatieplicht.
6. Binnen het NTC Firenze 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.
7. Het NTC Firenze 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 te nemen maatregelen.
8. Informatiebeveiliging en privacy is bij het NTC Firenze een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
9. Het NTC Firenze 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.
10. Het NTC Firenze 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.
11. Het NTC Firenze zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen

1.4 Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

1.4.1 Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- La legge 28 marzo 2003 no. 53

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

1.4.2 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 staan 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 docenten) 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.

1.4.3 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. IBP Bijlage 1 (§ **Error! Reference source not found.**) geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

1.4.4 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor docenten. Verhoging van het IBP-bewustzijn is een verantwoordelijkheid van het bestuur als eindverantwoordelijke.

1.4.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen 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 betrouwbaarheidsaspecten die van belang zijn.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op

informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

1.4.6 Incidenten en datalekken

Alle docenten die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij de coördinator gegevensbescherming (zie IBP - annex privacy verklaring leerlinggegevens.docx).

Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

1.4.7 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 geïnventariseerde risico's;
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan.

Daarnaast kent het NTC Firenze 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. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

1.4.8 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun docenten aanspreken in geval van tekortkomingen.

1.5 Organisatie - Wie doet wat?

Het bestuur van het NTC Firenze is verantwoordelijk voor de organisatie, controle en naleving van het IBP. Gezien de kleine omvang van de stichting (organisatie) en het ontbreken van ondersteunende bedrijfsfuncties, wordt geen onderscheid gemaakt naar strategische, tactische of operationele rollen en/of proceseigenaren.

De docenten zijn verantwoordelijk voor het beheer van data met betrekking tot het onderwijs.

2 Reglementen en protocollen

2.1 Privacyreglement

Het privacyreglement is opgenomen in het document *IBP - annex privacyreglement.docx*.

Naast het privacyreglement is een toelichting uitgewerkt waarin wordt beschreven wat (welke bewerkingen) met persoonsgegevens worden uitgevoerd. Deze toelichting is opgenomen in het document *IBP - annex privacy verklaring leerlinggegevens.docx*.

2.2 Protocol beveiligingsincidenten en datalekken

Het protocol beveiligingsincidenten en datalekken is opgenomen in het document *IBP - annex protocol incidenten en lekken.docx*.

3 Toestemming

Er wordt toestemming gevraagd aan de ouders van leerlingen voor het gebruik van persoonlijke gegevens (ook foto's gelden als persoonsgegeven). Er wordt onderscheid gemaakt tussen verschillende toestemmingen, welke ieder jaar opnieuw worden gevraagd als onderdeel van de inschrijving van leerlingen.

- Toestemming voor gebruik van persoonlijke gegevens voor administratieve doeleinden van de school (niet jaarlijks maar eenmalig bij de eerste inschrijving):
    - Leerling + voortgang administratie;
    - Contact voor diverse activiteiten door school georganiseerd;
- Toestemming voor het delen van persoonlijke gegevens (telefoonnummer in whatsapp groep, e-mail adres) voor:
    - Afstemming over af te drukken materialen;
    - Logistieke mededelingen;
    - Delen van foto's;
- Toestemming voor het plaatsen foto's;
    - Aparte toestemming wordt gevraagd voor het plaatsen van foto's op folders, sociale media en/of website.

De jaarlijks afgegeven toestemmingen kunnen worden ingetrokken.

Zie ook *IBP - annex privacy reglement.docx*.

4 Richtlijnen, afspraken en informatieplicht

De betrokkene heeft het 'recht om te worden vergeten' door het volledig wissen van de persoonsgegevens, tenzij er een wettelijke bewaarplicht geldt of het verwijderen in strijd is met de vrijheid van meningsuiting. Voor het onderwijs is dit recht minder relevant omdat er veel wettelijke bewaartermijnen gelden.

In principe geldt voor leerling gegevens een standaard bewaartermijn van 2 jaar nadat de leerling de school verlaten heeft. Er is op deze regel echter een aantal uitzonderingen:

- Gegevens over verzuim en in- en uitschrijving (5 jaar na vertrek)
- Gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen (3 jaar na vertrek)
- Adresgegevens van (oud-)leerlingen mag de school bewaren voor het organiseren van reünies.

Transparantie en rechten betrokkenen

(Deze paragraaf bevat een modeltekst van stichting kennisnet)

Transparantie is een belangrijke privacy-waarde. Je betrekt ouders en leerling actief. Je legt uit, vertelt welke gegevens je wilt vastleggen of verstrekken aan het samenwerkingsverband, of een derde, en waarom. Dit geldt ook voor de informatieoverdracht tussen scholen bij een overstap.

Je stelt ouders en leerling in staat om bezwaren te uiten en hun rechten uit te oefenen. Deze rechten zijn vastgelegd in de wet. De betrokkenen hebben de volgende rechten:

- Recht op informatie houdt in dat de leerling en/of zijn ouders (de betrokkene) vooraf in begrijpelijke taal actief en laagdrempelig worden geïnformeerd over welke gegevens met welk doel worden verwerkt en wat de rechten van de leerling zijn;
- Recht op inzage in en correctie van de persoonsgegevens. De betrokkene heeft het recht op inzage van zijn gegevens en het verbeteren of aanvullen van ontbrekende of verkeerd vastgelegde persoonsgegevens;
- Recht op verwijdering van de persoonsgegevens die niet (langer) nodig zijn om de vastgestelde doelen te behalen. Het gaat alleen om gegevens die niet noodzakelijk zijn, of als het opslaan van die gegevens in strijd is met de wet. Een leerling kan dus niet vragen om zijn ‘1’ voor een overhoring te 'verwijderen’ op grond van privacywetgeving;
- Recht van verzet tegen verwerking van persoonsgegevens bij de grondslag gerechtvaardigd belang, of verzet tegen direct marketing en profilering. De betrokkene kan verzet instellen tegen een verwerking van zijn persoonsgegevens die plaats vond op grond van een gerechtvaardigd belang. De school maakt een afweging van het privacybelang van de leerling, tegenover het belang van de school om gegevens wél te gebruiken;
- De leerling en/of zijn ouders hebben het recht om bij toestemming, ook een beperkte toestemming te geven of toestemming te onthouden voor een onderdeel van de verwerking (granulaire toestemming);
- De leerling en/of zijn ouders hebben het recht dat verbeteringen, aanvullingen of verwijderingen aan alle andere partijen worden doorgegeven aan wie een organisatie de persoonsgegevens van betrokkene heeft verstrekt;
- Het recht op ‘bevriezing van de verwerking’ van zijn gegevens;
- De betrokkene heeft het ‘recht om te worden vergeten’ door het volledig wissen van de persoonsgegevens, tenzij er een wettelijke bewaarplicht geldt of het verwijderen in strijd is met de vrijheid van meningsuiting. Voor het onderwijs is dit recht minder relevant omdat we veel wettelijke bewaartermijnen gelden;
- In geval van toestemming of een overeenkomst met de betrokkene, heeft de betrokkene het recht op dataportabiliteit als de verwerking van persoonsgegevens plaatsvindt op de grondslag toestemming. Scholen werken niet veel met toestemming, daarom is dit recht minder relevant;
- Recht op melding datalek: bij een datalek hebben de leerling en/of zijn ouders recht om daarover te worden geïnformeerd indien zij daar een zwaarwegend belang bij hebben.

5 Verwerkersovereenkomsten

Het NTC Firenze maakt geen gebruik van geautomatiseerde systemen voor leerlingenadministratie. Er wordt gebruik gemaakt van standaard Office applicaties, bestanden worden gedeeld via een gedeeld Dropbox account.

Er zijn geen verwerkersovereenkomsten afgesloten met derde partijen. Mochten er in de toekomst met leveranciers (van leermiddelen) die werken met privacygevoelige gegevens van leerlingen gewerkt gaan worden dan zullen verwerkersovereenkomsten worden afgesloten, en hierover zal worden gecommuniceerd naar ouders. Voor de partijen die het convenant getekend hebben, geldt dat ze de modelovereenkomst 3.0 kunnen tekenen.

6 Sociale media en email

Voor het bestuur, docenten, leerlingen en de ouders gelden de volgende regels voor sociale media (inclusief Whatsapp en Facebook) en email:

- Geen persoonlijke gegevens (inclusief herkenbare foto's) van docenten, leerlingen en ouders verspreiden tenzij hier expliciet toestemming voor is gegeven door de betreffende ouders in de jaarlijkse toestemmingsprocedure;
- Gezien de kleinschalige aard was het gebruikelijk binnen NTC om emails naar de hele vereniging in "To" of "CC" te schrijven. Vanaf 2021 is het beleid om de geadresseerden in de bcc (blind carbon copy) te zetten zodat de emailadressen van de andere geadresseerden niet zichtbaar zijn.
- Bij twijfel of problemen: neem contact op met het bestuur of met de schoolleider.

7 Functionaris Gegevensbescherming

Bij de vaststelling van dit beleidsplan, heeft het bestuur van het NTC ervoor gekozen geen Functionaris Gegevensbescherming (FG) aan te stellen (definitie FG). Hoewel een FG verplicht is voor onderwijsinstellingen (artikel 3 AVG) zijn de volgende argumenten hiervoor in overweging genomen:

- De zeer kleine omvang van de organisatie (3 bestuursleden, 2 leerkrachten) en het ontbreken van administratief personeel.
- De zeer kleine omvang van het aantal leerlingen (16 inschrijvingen op peildatum 1 oktober 2020).
- Het ontbreken van geautomatiseerde gegevensverwerking, systemen voor leerlingenadministratie of toepassing van informatiesystemen tijdens het uitvoeren van lessen.
- De zeer beperkte hoeveelheid gegevens die door de stichting wordt verzameld en/of verwerkt. Er is geen sprake van verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen.
- Het betreft een stichting die een dagdeel onderwijs verzorgt. Deze stichting kwalificeert echter op basis van bovenstaande argumenten ons inziens niet als onderwijsinstelling, noch als publieke organisatie.

In de *IBP - annex privacy verklaring leerlinggegevens.docx* is wel een contactpersoon gegevensbescherming benoemd.

8 5 vuistregels voor privacy 2.0

(Deze bijlage bevat een tekst van stichting kennisnet)

Privacy is een lastig en vaag begrip. Privacy op school gaat over de bescherming van gegevens over leerlingen, hun ouders en docenten. Dit wordt geregeld in de Wet bescherming persoonsgegevens. Per 25 mei 2018 wordt deze wet vervangen door de Europese Algemene Verordening Gegevensbescherming (AVG) die in heel Europa van toepassing wordt. Deze nieuwe wetgeving stelt hogere en aanvullende eisen aan privacy. In deze 5 vuistregels voor po, vo en mbo (versie 2.0) worden de belangrijkste (nieuwe) uitgangspunten voor het verantwoord omgaan met persoonsgegevens samengevat.

Denk bij het verzamelen, registreren en verwerken van persoonsgegevens altijd aan de 5 vuistregels:

1. Doel en doelbinding
    a. Heb ik vooraf een doel voor de verwerking van persoonsgegevens vastgesteld? Worden de persoonsgegevens alleen gebruikt voor dat doel dat ik vooraf heb vastgelegd?
2. Grondslag
    a. Is er minimaal een wettelijke grond voor de verwerking?
        i. Ik heb toestemming van leerling of ouders
        ii. De gegevens zijn nodig voor de uitvoering van een overeenkomst
        iii. Het verwerken van deze gegevens is wettelijk verplicht
        iv. De verwerking van gegevens is nodig voor het uitvoeren van onze publiekrechtelijke taak
        v. Er is een gerechtvaardigd belang dat ik kan uitleggen aan (de ouders van) de leerlingen.
3. Dataminimalisatie
    a. Gebruik ik alleen die gegevens die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? Kan ik met minder of bijvoorbeeld anonieme gegevens werken? Bewaar ik de gegevens niet langer dan nodig?
4. Transparantie
    a. Heb ik de leerling of zijn ouders vooraf helder geïnformeerd over het doel van de gegevensverwerking? Heb ik uitgelegd welke gegevens worden gebruikt en met wie deze worden gedeeld?
5. Integriteit
    a. Kloppen de persoonsgegevens die ik gebruik nog steeds? Zijn de gegevens op het juiste moment, op de juiste plaats en voor de juiste mensen beschikbaar? Heb ik onjuiste gegevens gecorrigeerd of verwijderd?