Privacybeleid
Stichting Nutsscholen Breda

“Bewust en transparant”

Inhoudsopgave

1. Inleiding

Met de komst van steeds meer diensten die buiten de scholen aangeboden worden, sociale media en kwalijke voorbeelden bij het gebruik van internet in het onderwijsveld, wordt de noodzaak om een goed privacybeleid te formuleren voor de Stichting Nutsscholen Breda, steeds groter. Er is ook een wet (Wet bescherming persoonsgegevens) die ons dat verplicht. De vertaling van de wet voor het onderwijs zit voor een belangrijk deel in het convenant digitale leermiddelen.

In het verleden werden gegevens van leerlingen en medewerkers op papier bijgehouden en bewaard in een veilige ruimte binnen de school. Er was minder noodzaak om gegevens te beschermen tegen buitenaf dan nu; er werden immers geen gegevens via internet uitgewisseld.
Nu worden onze bestanden op een server opgeslagen, onze leerling- en personeelsgegevens staan op een online dienst, educatieve content wordt aangeboden door derde partijen en bij sociale media is de derde partij vaak erg opdringerig.

Daarbij komt ook dat de buitenwereld veranderd is. Vroeger was een hek om de school en een alarmsysteem afdoende om ongewenste personen buiten te houden. Nu zullen we ook een “digitaal hek” moeten maken.

De nieuwe mogelijkheden op ICT gebied hebben ons veel vooruitgang gebracht. Er is in het verleden echter onvoldoende nagedacht om de gegevens te beschermen. In het onderwijs is immers een gedachte dat we voor de leerlingen alleen het beste willen. We zien echter dat de buitenwereld veel meer binnen de school kan komen dan gedacht. We moeten er voor zorgen dat we daar zorgvuldiger in worden. Het belangrijkste in de bescherming van privacy van onze leerlingen en medewerkers is daarom bewustwording. Bewust zijn dat een wachtwoord veilig moet zijn, bewust dat data op een veilige plaats wordt opgeborgen, bewust dat een eenmaal geplaatste foto op Facebook nooit meer te verwijderen valt.

In dit beleidsstuk wordt aandacht besteed aan wat de Wet Bescherming Persoonsgegevens (Wbp) ons voorschrijft en hoe dat vertaald is naar het privacyreglement en wat dat voor betekenis dit heeft voor de volgende componenten:

1. Beveiliging van ons netwerk
2. Leveranciers van ICT software en Convenant digitale leermiddelen
3. Foto’s op school
4. Hanteren van sociale media
5. Privacy in digitale (overstap)dossiers

We zijn samen op alle vlakken verantwoordelijk voor het waarborgen van de privacy van onze leerlingen en medewerkers en we dienen daar transparant over te zijn. En daar moeten we ons van bewust zijn.

Een opsomming van het in dit stuk gebruikte bronmateriaal is terug te vinden is aan het laatste hoofdstuk.

2. Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) geeft regels ter bescherming van de privacy van burgers.
De persoonsgegevens van een gemiddelde burger komen in honderden bestanden voor, dus ook in het onderwijs.

De Wbp geeft de burger bepaalde rechten, zoals het recht om te weten wat er met zijn persoonsgegevens gebeurt. De burger mag zijn gegevens te allen tijde inzien en mag ook verzoeken tot onder andere correctie van zijn gegevens en bezwaar maken tegen de verwerking van zijn persoonsgegevens.

Organisaties die persoonsgegevens verwerken hebben bepaalde plichten. Zo mogen persoonsgegevens, kort gezegd, verzameld en verder verwerkt worden, mits daarvoor welbepaalde en uitdrukkelijk omschreven doelen zijn en deze doelen gerechtvaardigd zijn door bijvoorbeeld toestemming van de betrokken burger. Ook moeten zij - uitzonderingsgevallen daargelaten - de burger laten weten wat zij met zijn gegevens (gaan) doen.

Rollen:
Vanuit de context van de wet worden drie rollen onderscheiden:

Betrokkene	Verantwoordelijke	Bewerker
De natuurlijke persoon over wie de gegevens wordt verzameld. Bij personen onder de 16 jaar zijn dat de ouders of rechtsgeldige vertegenwoordiger(s).	Directie/bestuur van de organisatie die de gegevens verzamelt.	De organisatie die namens de verantwoordelijke de gegevens bewerkt.
Context school: Leerlingen Personeel	Context school: Bevoegd gezag	Context school: Leveranciers van ICT systemen

Bij het aangaan met een relatie die gegevens bewerkt, dient volgens de Wbp gehandeld te worden. De volgende vijf vuistregels zijn dan altijd aan de orde:

1. ***Doel***
   Heb ik vooraf een doel voor de verwerking van de persoonsgegevens vastgesteld?
2. ***Doelbinding***
   Worden de persoonsgegevens alleen gebruikt voor het doel dat ik vooraf heb vastgelegd?
3. ***Grondslag***
   Is er minimaal één wettelijke grondslag voor de verwerking?
   --Er is toestemming van leerling (ouders) en/of personeel
   --De gegevens zijn nodig voor de uitvoering van de overeenkomst
   --Het verwerken van de gegevens is wettelijk verplicht
   --De verwerking van gegevens is nodig voor het uitvoeren van onze publiekrechtelijke taak
   --Er is een gerechtvaardigd belang dat ik kan uitleggen aan (de ouders van) de leerlingen of personeel.
4. ***Dataminimalisatie***
   Worden alleen die gegevens gebruikt die noodzakelijk zijn om het vastgesteld doel te verwezenlijken en worden ze niet langer bewaard dan nodig?

5. ***Transparantie***
   Zijn de ouders (of leerling) of personeel vooraf geïnformeerd over het doel van de gegevensverwerking en is ze uitgelegd, welke gegevens worden gebruikt en met wie ze worden gedeeld?

Hiermee is de Wbp een hele duidelijke reden waarom scholen en stichtingen vanaf 2016 duidelijk in kaart moeten brengen hoe men hier mee omgaat, erover communiceert en vastlegt o.a. als uitwerking van de Wet bescherming persoonsgegevens (Wbp).

Dit is een belangrijke basis voor een document dat na vaststelling geldend is als privacyreglement en -beleid van Stichting Nutsscholen Breda.

3. Privacyreglement Stichting Nutsscholen Breda

1. Aanhef

Dit reglement is voor Stichting Nutsscholen Breda, gevestigd Hooilaan 1, 4816 EM Breda.

2. Definities

Persoonsgegevens: Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

Verwerking van persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
Bijzonder persoonsgegeven
Een persoonsgegeven dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid of zijn gezondheid;
Betrokkene
Degene op wie een persoonsgegeven betrekking heeft al dan niet vertegenwoordigd door diens wettelijk vertegenwoordiger;
Wettelijk vertegenwoordiger
Indien de betrokkene de leeftijd van zestien jaren nog niet heeft bereikt, wordt de betrokkene vertegenwoordigd door zijn wettelijk vertegenwoordiger. Meestal zal dit een ouder zijn maar het kan hier ook gaan om een voogd;
Verantwoordelijke
De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Dat wil zeggen de gemeente of (openbare of privaatrechtelijke) rechtspersoon waar de stichting onder valt: het bevoegd gezag. Wanneer er in dit reglement gesproken wordt over de Verantwoordelijke dan wordt daarmee het bevoegd gezag van Stichting Nutsscholen Breda bedoeld.
Bewerker
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
Derde
Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;
Stichting
De verantwoordelijke onderwijsinstelling / bevoegd gezag.

3. Reikwijdte en doelstelling

1. Dit reglement stelt regels over de verwerking van persoonsgegevens van leerlingen en personeelsleden van de stichting.
2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door Stichting Nutsscholen Breda worden verwerkt. Dit reglement heeft tot doel:
a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens;
b. vast te stellen welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt;
c. de zorgvuldige verwerking van persoonsgegevens te waarborgen;
d. de rechten van betrokkene te waarborgen.

4. Doelen van de verwerking van persoonsgegevens

Bij de verwerking van persoonsgegevens houdt Stichting Nutsscholen Breda zich aan de relevante wetgeving waaronder de Wet bescherming persoonsgegevens.

Doelen

De verwerking van persoonsgegevens vindt plaats voor:

a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, deelnemers of studenten, dan wel het geven van studieadviezen;
b. het vervullen van de werkgeversrol;
c. het verstrekken of ter beschikking stellen van leermiddelen;
d. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld, onder a en b, alsmede informatie over de leerlingen, deelnemers of studenten, bedoeld in het eerste lid, op de eigen website;
e. het bekendmaken van de activiteiten van de instelling of het instituut op de eigen website;
f. het berekenen, vastleggen en innen van inschrijvingsgelden, stichting- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buiten-stichtingse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen;
g. het behandelen van geschillen en het doen uitoefenen van accountantscontrole;
h. het onderhouden van contacten met oud-leerlingen of oud-personeelsleden;
i. de uitvoering of toepassing van een andere wet.

5. Vrijstelling meldingsplicht

De in artikel 4 genoemde gegevensverwerkingen vallen onder het vrijstellingsbesluit Wbp en hoeven niet worden aangemeld bij het CBP.

6. Doelbinding

Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. De stichting verwerkt niet meer gegevens dan noodzakelijk is om die vastgestelde doelen te bereiken.

7. Soorten gegevens

De door de stichting gebruikte categorieën van persoonsgegevens worden in bijlage 1 opgesomd.

8. Grondslag verwerking

Verwerking van persoonsgegevens gebeurt alleen op grond van:

a. Toestemming: in het geval de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend

b. Overeenkomst: in het geval de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst

c. Wettelijke verplichting: in het geval de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de Stichting Nutsscholen Breda onderworpen is

d. Publiekrechtelijke taak: in het geval de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt

e. Gerechtvaardigd belang: Als gevolg en uitwerking van de wet.

9. Bewaartermijnen

Stichting Nutsscholen Breda bewaart de gegevens niet langer dan dat zij noodzakelijk zijn voor het vervullen van het doel waarvoor zij zijn verkregen, tenzij er een andere wettelijke verplichting is die het langer bewaren van de gegevens verplicht stelt.

10. Toegang

De Stichting Nutsscholen Breda verleent slechts toegang tot de in de administratie en systemen van de stichting opgenomen persoonsgegevens aan:
a. de bewerker en de derde die onder rechtstreeks gezag van de Stichting Nutsscholen Breda staat;
b. de bewerker die gemachtigd is om persoonsgegevens te verwerken;
c. derden die op grond van de wet toegang moet worden verleend, waarbij alleen toegang wordt verleend aan de gegevens waartoe volgens de wet toegang toe moet worden gegeven.

11. Beveiliging en geheimhouding

a. De Stichting Nutsscholen Breda neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
b. De Stichting Nutsscholen Breda zorgt dat medewerkers niet meer inzage of toegang hebben tot de persoonsgegevens dan zij strikt noodzakelijk nodig hebben voor de goede uitoefening van hun werk.
c. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging. Daarbij houdt de stichting rekening met de concrete risico's die van toepassing kunnen zijn op de verwerkte persoonsgegevens.
d. Iedereen die betrokken is bij de uitvoering van dit reglement, en daarbij de beschikking krijgt over persoonsgegevens die vertrouwelijk zijn of geheim moeten worden gehouden (zoals bijvoorbeeld zorggegevens), en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die persoonsgegevens daarvan.

12. Verstrekken gegevens aan derden

Wanneer daartoe een wettelijke plicht bestaat moet Stichting Nutsscholen Breda de persoonsgegevens verstrekken aan derden. Het verstrekken van persoonsgegevens aan derden kan ook plaatst vinden na toestemming van de betrokkene.

13. Sociale media

Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het 'sociale-mediaprotocol' van Stichting Nutsscholen Breda .

14. Rechten betrokkenen

1. De Wbp geeft de betrokkene een aantal rechten. Stichting Nutsscholen Breda erkent deze rechten en handelt in overeenstemming met deze rechten.

Inzage

Elke betrokkene heeft recht op inzage van de door Stichting Nutsscholen Breda verwerkte persoonsgegevens die op hem/haar betrekking hebben. Stichting Nutsscholen Breda mag voor het inwilligen van dit verzoek een kostprijs verbinden van maximaal € 5,-. Wanneer het verzoek wordt afgewezen dan worden er geen kosten in rekening gebracht. Stichting Nutsscholen Breda kan vragen om een geldig identiteitsbewijs ter verificatie van de identiteit van de verzoeker.

Verbetering, aanvulling, verwijdering en afscherming
Betrokkene kan een verzoek doen tot verbetering, aanvulling, verwijdering of afscherming van zijn persoonsgegevens, tenzij dit onmogelijk blijkt of een onredelijke inspanning zou vergen.
Verzet
Voor zover Stichting Nutsscholen Breda persoonsgegevens gebruikt op de grond van artikel 4 onder e en f, dan kan de betrokkene zich verzetten tegen verwerking van persoonsgegevens op basis van diens persoonlijke omstandigheden.
Termijn
Stichting Nutsscholen Breda dient binnen een termijn van 4 weken (*Niet vallende in de zomervakantie)* na ontvangst van een verzoek hieraan schriftelijk gehoor te geven dan wel deze schriftelijk, gemotiveerd af te wijzen.
De stichting kan de betrokkene laten weten dat er meer tijd nodig en deze termijn verlengen met maximaal 4 weken.
Uitvoeren verzoek
Indien het verzoek van de betrokkene wordt gehonoreerd, draagt Stichting Nutsscholen Breda zorg voor het zo spoedig mogelijk doorvoeren van de verzochte wijzigingen.
Intrekken toestemming
Voor zover voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming ten allen tijden door de wettelijk vertegenwoordiger worden ingetrokken.

15. Transparantie

1. De Stichting Nutsscholen Breda informeert de betrokkene over de verwerking van zijn persoonsgegevens. Indien het type verwerking dat vraagt, informeert de stichting iedere betrokkene apart over de details van die verwerking.
2. De Stichting Nutsscholen Breda informeert de betrokkene – op hoofdlijnen – ook over de afspraken die gemaakt zijn met derden en bewerkers die persoonsgegevens van de betrokkene ontvangen.

16. Klachten

1. Wanneer men van mening is dat het doen of nalaten van Stichting Nutsscholen Breda niet in overeenstemming is met de Wbp of zoals dat is uitgewerkt in dit reglement is, dan dient u zich te wenden tot de directeur-bestuurder van de Stichting Nutsscholen Breda .
2. Overeenkomstig de Wpb kan de betrokkene zich eveneens wenden tot de rechter of het College bescherming persoonsgegevens.

17. Onvoorziene situatie

Indien er zich een situatie voordoet die niet beschreven is in dit reglement dan neemt de verantwoordelijke de benodigde maatregelen.

18. Wijzigingen reglement

1. Dit reglement treedt in na vaststelling van het bestuur en (G)MR. De verantwoordelijke maakt dit reglement openbaar via bestuursbesluit van het bestuur van de Stichting Nutsscholen Breda.
De verantwoordelijke heeft het recht dit reglement, met instemming van de (G)MR, te wijzigingen.

19. Slotbepaling

Dit reglement wordt aangehaald als “het privacyreglement” van Stichting Nutsscholen Breda en treedt in werking op xx-xx-2016. Na passeren en goedkeuring bij/door het bestuur van de Stichting Nutsscholen Breda en GMR

Uitleg van de termen is toegevoegd als bijlage 1

3.1 Overzicht van categorieën gebruikte persoonsgegevens

Omschrijving en opsomming categorieën Persoonsgegevens die gebruikt worden:
Bijvoorbeeld:
a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de betrokkene;
b. het persoonsgebonden nummer (BSN);
c. nationaliteit, land van herkomst;
d. gegevens als bedoeld onder a alsmede opleidingsniveau, land van herkomst, en beroep van de wettelijk vertegenwoordiger of verzorger van de leerling;
e. gegevens betreffende de gezondheid of het welzijn van de leerling voor zover die noodzakelijk zijn voor de ondersteuning;
f. gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor de stichting, het onderwijs of de te geven ondersteuning;
g. gegevens betreffende de aard en het verloop van het onderwijs en ondersteuning, alsmede de behaalde studieresultaten;
h. stichtings(school)gegevens (waaronder naam stichting, naam zorgcoördinator/mentor/ intern begeleider, klas/groep waarin de leerling zit, tijdstip van inschrijving bij deze stichting, naam van de indiener van de aanmelding bij het samenwerkingsverband, schoolloopbaan en rapportage vanuit primair en voortgezet onderwijs);
i. aanleiding voor de aanmelding bij het samenwerkingsverband, relevante screenings- en onderzoeksgegevens en omschrijving van de problematiek die aan de orde is;
j. activiteiten die door de stichting zijn ondernomen rond de betreffende leerling, alsmede de resultaten hiervan;
k. bestaande of (relevante) afgesloten hulpverleningscontacten en de namen van contactpersonen;
l. relevante persoonsgegevens die door externe partijen worden verstrekt met betrekking tot de aangemelde problematiek van de betreffende leerling;
m. relevante financiële gegevens over bijvoorbeeld schoolgeld.

4. Beveiliging van ons netwerk

Ons netwerk is zo veilig mogelijk ingericht. De architectuur is zodanig dat we slechts één gateway naar buiten hebben. Dat wil zeggen dat we eigenlijk maar één poort hoeven te bewaken. In de oude situatie hadden de scholen zelf een server in het pand staan. Alle servers zijn in 2014 vervangen door een centrale oplossing. De glasvezelverbindingen die de scholen aan het centrale datacenter verbinden is een alleen voor de SNB toegewezen verbinding. Over deze glasvezelverbinding gaat geen enkele bit data van een andere partij. Fysiek is dit geheel gescheiden.

Omdat er maar één poort is, hoeft ook alleen maar deze poort beveiligd te worden. In ons geval gebeurt dit met een extra zware firewall. Ook op de locaties van de scholen zelf is nog een tweede obstakel aangebracht door lokaal nog een extra hindernis te maken. Dit is niet strikt noodzakelijk, maar hoe meer hindernissen er voor externen worden aangebracht, hoe minder aantrekkelijk het wordt voor een externe indringer om een hackaanval te plaatsen.

Onze data zijn via een remote applicatie voor alle medewerkers op afstand te benaderen. De data die we in eigen beheer hebben, blijven echter fysiek in ons datacenter in Eindhoven (en backups in 's-Hertogenbosch). We hebben een zogenaamde private cloud gemaakt. Een zelfde soort cloudopslag als OneDrive of DropBox, alleen dan ongelimiteerd, met een backupsysteem en binnen de eigen organisatie.
Sinds het voorjaar van 2016 is My Learning (onze elektronische leeromgeving) overgebracht naar ons eigen datacenter. Alle data die hierin wordt opgeslagen zijn beveiligd volgens onze normen. Via My Learning zijn data uitstekend te benaderen op alle mogelijke apparaten met een internetverbinding. Dit is zo ingericht omdat het sluiten van een bewerkersovereenkomst met een buitenlands bedrijf ook andere wetgeving met zich meebrengt. Door de data in eigen beheer te hebben, geldt hier de Nederlandse wetgeving over en kunnen we de privacy volgens deze normen waarborgen.

Privacy:
De wijze waarop we het netwerk hebben ingericht, is gericht op eigen beheer en het niet afhankelijk zijn van derde grote partijen. Ons netwerk wordt beheerd door VDN ICT, maar kan op ieder moment ook door een andere partij beheerd worden. Dit omdat wij eigenaar zijn van alle materialen.
Met de beheerpartij stellen we een bewerkersovereenkomst op.

Risico's vermijden:

Externe back-up:
Het is mogelijk dat gebruikers data op een externe dienstverlener stallen. DropBox of Onedrive zijn hier voorbeelden van. Deze diensten zijn gratis en heel gebruiksvriendelijk. Als SNB hebben we geen enkel zicht op de data die hier opgeslagen wordt. We kunnen de gebruikers ook geen ondersteuning bieden door middel van back-up of extra dataopslag. Aangezien deze data veelal op Amerikaanse servers worden opgeslagen staan deze data ook bloot aan bemoeienissen van overheden. Hoewel in een Europees convenant is omschreven dat deze softwareleveranciers niet in de data zullen kijken, zullen ze wel degelijk de data afstaan aan een overheid als die daar om verzoekt. Als alternatief bieden we My Learning aan.

Wachtwoorden:
De zwakste schakel in de beveiliging van ons netwerk is de gebruiker. De gebruiker heeft vaak een veel te makkelijk wachtwoord. Aan de ene kant is dat heel snel te kraken door een extern stukje software. Maar vaak is dat niet nodig. Men kan het wachtwoord ook heel makkelijk achterhalen

omdat het ergens op geschreven is en makkelijk vindbaar is. De beroemde “geeltjes” die aan de monitor geplakt zijn bijvoorbeeld.
De gebruiker vergeet doorgaans ook zijn systeem op slot te zetten als hij zijn werkplek even verlaat. Het systeem blijft dan met de rechten van de gebruiker open staan en iedereen heeft de mogelijkheid om vertrouwelijke informatie in te zien.

Mobiele gegevensdragers en harddisks:
USB sticks met privacygevoelige gegevens van leerlingen of medewerkers worden niet gebruikt. Via My Learning zijn deze gegevens uitstekend te benaderen op iedere plek met een internetverbinding.
Mobiele harddisks voor archiefdoeleinden blijven ten alle tijden in een afsluitbare ruimte op school.
Laptops of andere draagbare apparaten met daarop privacygevoelige gegevens worden beveiligd met het domeinwachtwoord van de SNB.
Bij het afschrijven en verwijderen van defecte computers of laptops, worden de harddisks leeggemaakt of verwijderd uit het systeem. Deze harddisks blijven in school of worden door een erkend destructiebedrijf vernietigd.

E-mail:
Om e-mailpartners op de hoogte te brengen en personen naar wie foutief een e-mail is verstuurd te verzoeken de e-mail te negeren en te verwijderen, is het verstandig voor iedere werknemer om een disclaimer mee te sturen.

De e-maildisclaimer is toegevoegd als bijlage 2.

Advies op basis van voorgaande:
De noodzakelijke verbeteringen ten aanzien van de beveiligingsrisico’s zijn:

--Opstellen bewerkersovereenkomst met VDN ICT
--Aanpassing wachtwoordbeleid
--Aanpassing beleid om werkstation af te sluiten (te locken)
--Invoeren van een e-maildisclaimer.

5. Convenant Digitale Onderwijsmiddelen en Privacy

Het ‘Convenant Digitale Onderwijsmiddelen en Privacy – Leermiddelen en Toetsen’ vertaalt de Wet bescherming persoonsgegevens naar de onderwijspraktijk. Het bevat afspraken over het omgaan met persoonsgegevens bij het gebruik van digitale leermiddelen en toetsen. Dankzij het convenant weten scholen en aanbieders wat ze over en weer van elkaar mogen verwachten, zijn de afspraken werkbaar in de praktijk en heeft iedereen dezelfde gemeenschappelijke uitleg bij deze afspraken.

5.1 Regie bij de school

Bij de afspraken staat voorop dat de school de regie heeft. De school is verantwoordelijk voor de zorgvuldige omgang met de persoonsgegevens van de leerlingen en de communicatie naar ouders. Hierbij hoort ook het maken van goede afspraken met aanbieders. Een school staat hier niet alleen in. De partijen bij het convenant hebben een gemeenschappelijke en gedeelde zorg om de school in staat te stellen deze verantwoordelijkheid vorm te geven.

5.2 De afspraken in de praktijk

De PO-Raad en de VO-raad hebben het convenant ondertekend namens alle aangesloten schoolbesturen. Aanbieders tekenen individueel het convenant en passen de afspraken toe in hun bewerkersovereenkomsten met scholen. Hiervoor kunnen zij de modelbewerkersovereenkomst gebruiken.

6. Leveranciers van ICT Software

Persoonsgegevens uitwisselen met uitgevers en andere leveranciers is vaak nodig. De Wbp geeft een aantal spelregels waarbinnen de school het wettelijke recht heeft om persoonsgegevens beschikbaar te stellen aan die leveranciers. Belangrijk is dat er met elke leverancier – voor de uitwisseling van gegevens – juridische afspraken worden gemaakt over wat de leverancier wél en niet mag met de persoonsgegevens. Deze afspraken worden vastgelegd in een contract dat we een bewerkersover-eenkomst noemen. Zo’n bewerkersovereenkomst is wettelijk verplicht. Het belangrijkste uitgangspunt in deze bewerkersovereenkomst is dat de bewerker (leverancier) alleen verwerkingen uitvoert in opdracht van de school. De leverancier mag de ontvangen gegevens niet voor iets anders gebruiken, de data doorverkopen of zelf contact opnemen met de ouders om bijvoorbeeld reclame te maken voor extra lesmateriaal. Meestal nemen leveranciers zelf het initiatief om een bewerkersovereenkomst op te stellen, maar volgens de Wbp blijft de school zelf verantwoordelijk voor de aanwezigheid en inhoud van de overeenkomst.

6.1 Regie over gegevens

In 2015 hebben de PO-Raad, VO-raad, uitgevers (GEU), softwareleveranciers (vDOD) en distributeurs van digitaal leermateriaal (KBb-e) het convenant ‘Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen’ (zie verder) ondertekend. Dit om scholen te ontzorgen en ze te helpen om de juiste afspraken te maken. Alle leveranciers die bij deze partijen zijn aangesloten, leveren op dit moment gezamenlijk zo’n 95 procent van alle beschikbare producten voor scholen. Dit convenant zorgt ervoor dat de scholen de regie hebben over wat er gebeurt met de gegevens die worden verwerkt bij het gebruik van digitale leermiddelen. Het convenant concretiseert hiermee veel verplichtingen voor scholen die voortvloeien uit de Wbp.

6.2 Modelbewerkersovereenkomst

Bij het convenant hoort een ‘Modelbewerkersovereenkomst’. Hierin maakt de school met de leverancier afspraken over welke gegevens de leverancier mag gebruiken. In de overeenkomst staat ook welke beveiligingsmaatregelen de leverancier treft om de veiligheid van de verwerkte persoonsgegevens te waarborgen. Deze afspraken zijn juridisch afdwingbaar. Alle leveranciers die het convenant ‘Digitale Onderwijsmiddelen en Privacy — Leermiddelen en Toetsen’ hebben ondertekend, zijn verplicht om deze Modelbewerkersovereenkomst te gebruiken. Afwijken van dit model kán, maar is niet wenselijk. Door ondertekening van de overeenkomst bekrachtigen de school en de leverancier dat zij zich aan de afspraken houden die in het convenant staan beschreven.

6.3 Privacybijsluiter

Bij de Modelbewerkersovereenkomst hoort een bijlage A, de ‘privacybijsluiter’. Hierin leggen de partijen vast met welk doel de gegevensverwerking plaatsvindt, wat de dienstverlening van de leverancier omvat en wat de producteigenschappen zijn. Daarnaast staat er beschreven welke categorieën persoonsgegevens de leverancier verwerkt. De leverancier vult de bijsluiter in. De school gaat vanzelfsprekend na of alles klopt en besluit uiteindelijk om wel of niet akkoord te gaan met de voorgestelde afspraken.

6.4 Technische en Organisatorische Maatregelen

In de bijlage B ‘Technische en Organisatorische Maatregelen’, staan alle beveiligingsmaatregelen beschreven. De Modelbewerkersovereenkomsten zullen in de loop van het schooljaar 2015/2016 gebruikt gaan worden. Ook hiervoor geldt dat de leverancier deze bijlage invult en het aan de school is om deze te checken.
De Modelbewerkersovereenkomst ondersteunt scholen wanneer zij een contract aangaan met een leverancier. Door de brede dekking in de markt van digitale onderwijsmiddelen die de ondertekenaars van het convenant hebben, zullen de uitgangspunten van het convenant straks in de praktijk de norm zijn. De Modelbewerkersovereenkomsten (en bijlagen) zullen in de loop van het schooljaar 2015/2016 gebruikt gaan worden door leveranciers.

6.5 Aan de slag met de bewerkersovereenkomst

Elke school kan de Modelbewerkersovereenkomst eenvoudig gebruiken. In het model zelf hoeven alleen de (contact)gegevens van de school en de leverancier te worden ingevuld. In de bijsluiters staat de concrete informatie over het product dat de school wil gebruiken. De privacybijsluiter wordt door de leverancier gemaakt. Het is mogelijk dat de school moet kiezen om bepaalde (extra) gegevens te delen. Dit moet de school dan aankruisen, denk bijvoorbeeld aan extra opties in het digitaal leermiddel. In de tweede bijlage staat welke (extra) beveiligingsmaatregelen er genomen zijn. De school kan in deze bijlage ook aparte afspraken maken met de leverancier over de beveiliging.

De modelbewerkersovereenkomst is als bijlage 3 toegevoegd.

7. Nummervoorziening

Privacy is een belangrijk thema voor ouders, scholen, leveranciers en de politiek. Om de privacy van leerlingen optimaal te waarborgen en partijen alleen die gegevens te geven die nodig zijn om de onderwijsdienst succesvol te gebruiken, is de nummervoorziening bedacht. Kennisnet heeft vanuit het Doorbraakproject Onderwijs & ICT de opdracht gekregen de nummervoorziening te ontwikkelen en te realiseren.

7.1 Wat is de nummervoorziening?

De nummervoorziening is een landelijk project dat er voor zorgt ervoor dat betekenisloze identificatienummers uitgewisseld kunnen worden binnen de onderwijsketen, zonder dat er persoonsgegevens van leerlingen gedeeld worden met en tussen partijen. Het nummer is een pseudoniem, dit wil zeggen dat instanties en leveranciers geen persoonskenmerken uit dit nummer kunnen afleiden. Dit leidt tot een situatie waarin bijvoorbeeld de voortgang van leerlingen kan worden gevolgd door alleen die partijen (meestal de school) die daar ook recht toe hebben, waarbij de privacy van leerlingen optimaal gewaarborgd is.
Het doel van Kennisnet is om vanaf schooljaar 2016-2017 met deze voorziening te kunnen werken.

8. Foto's op school

Een foto waarop een leerling herkenbaar in beeld is, zegt iets over de leerling. De foto is een persoonsgegeven. Daarom is de Wbp van toepassing op gebruik van (pas) foto's waarop een of meerdere leerlingen herkenbaar in beeld zijn. Als de school die foto bijvoorbeeld op de website wil zetten, dan is daar geen andere grondslag voor mogelijk dan toestemming. Uit de praktijk blijkt dat scholen verschillend omgaan met toestemming vragen.

8.1 Vraag altijd toestemming

De Wbp geeft geen rechtvaardiging om foto's van leerlingen te publiceren zonder toestemming van de ouders. Als ouders dus geen toestemming hebben gegeven voor gebruik van foto's, dan zorgt de school ervoor dat die foto's ook écht niet gebruikt worden.
Er dient voor gezorgd te worden dat er altijd toestemming van de ouders is als er foto's, video's of persoonlijke informatie van en over leerlingen (en ouders) publiekelijk gedeeld wordt. Het is niet genoeg dat bijvoorbeeld in groep 1 éénmalig toestemming wordt gevraagd om foto's of informatie van leerlingen te gebruiken.
De Wbp gaat ervan uit dat de school altijd opnieuw om toestemming vraagt. Scholen kunnen ervoor kiezen om - uit praktisch oogpunt – toch éénmalig toestemming te vragen. De school moet de ouders er dan wel elk jaar op wijzen dat de school gebruik maakt van hun gegeven én dat ze bezwaar kunnen maken tegen foto's op de website. Dat is niet helemaal zoals de wetgever dit bedoelde, maar het komt wel tegemoet aan de bescherming van de privacy van de leerlingen. Het is een praktische oplossing voor ouders én school.
Verder moet de school specifieke toestemming vragen voor de manier waarop de foto's, video's en informatie worden gebruikt. Een algemene toestemming is niet voldoende. Er dient apart toestemming voor foto's op de website, in de nieuwsbrief, schoolgids, folder en voor sociale media gevraagd te worden.
Verder is het advies om toegang tot beeldmateriaal op de website van de school te beveiligen, waarbij ouders alleen toegang hebben met een code of wachtwoord. Dit gaat ongewenst meekijken tegen, door bijvoorbeeld mensen met verkeerde bedoelingen.

8.2 Delen via sociale media

Er zijn steeds vaker ouders die bewust geen foto's van hun kinderen willen (laten) delen op sociale media. Het is dus verstandig om hier apart toestemming voor te vragen (ook per sociaal medium). Wanneer een school een foto deelt via Facebook of Twitter gaat de school akkoord met de algemene voorwaarden van deze organisatie. Het is vervolgens moeilijker om zelf controle te hebben over wat er met deze foto gebeurt. Ook voor een folder, kalender of schoolgids kan het beste vooraf apart toestemming worden gevraagd.

8.3 Foto's maken door ouders op school

Het kan voorkomen dat ouders het vervelend vinden dat andere ouders foto's maken van hun kinderen.
Meestal overleggen deze ouders samen over het maken en gebruik van die foto's. Soms komen ouders er samen niet uit en dan wordt de school gevraagd om iets te regelen.
De school wil voor álle kinderen een veilige omgeving zijn, en niet een plek waar kinderen (en hun ouders) bang hoeven te zijn steeds te worden gefotografeerd. Het maken van foto's en video's op school kan moeilijk worden verboden, maar kan wel aan banden worden gelegd. Dit kan door bijvoorbeeld verwachtingen uit te spreken naar ouders over fotograferen tijdens een schoolactiviteit, of door ouders in de nieuwsbrief te vragen terughoudend te zijn met het maken en publiceren van foto's.
Mocht dat niet het gewenste effect hebben, dan kan de school regels voor het maken van foto's op school vastleggen in het privacyreglement of in een aparte gedragscode of een protocol.
Een schoolgebouw is niet zomaar een openbare plaats waar iedereen toegang toe heeft. De school kan aan het verlenen van toegang dus voorwaarden verlenen zoals de (extreme) regel dat fotograferen van leerlingen tijdens de les of in klas alleen is toegestaan door docenten.

Een voorbeeldbrief voor ouders met toelichting is toegevoegd als Bijlage 4.

9. Sociale Media op school

Internet en sociale media worden steeds vaker door leerlingen en docenten gebruikt. De informatie die online wordt gedeeld, bevat vaak persoonsgegevens: een foto, naam, gedrag, uitnodiging of gesprek. Is het niet in de les, dan is het wel op het schoolplein. Internet en sociale media maken daarmee onderdeel uit van het schoolklimaat.
Sinds 1 augustus 2015 zijn scholen wettelijk verplicht om te zorgen voor een sociaal veilig klimaat op school. 'Sociale veiligheid op internet' moet een vaste plek krijgen op school. Elke school moet een schoolveiligheidsplan met een pestprotocol hebben, eventueel aangevuld met een media- of gedragscode.

9.1 Internet- of Sociale mediaprotocol

In een mediaprotocol beschrijft een school wat er verwacht wordt van leerlingen op sociale media. Wat op het schoolplein gebeurt, gaat tegenwoordig tenslotte op sociale media verder. Men spreekt met elkaar af dat leerlingen geen filmpjes en foto's van elkaar delen als deze nadelig voor personen zijn. Het is ook een startpunt om leerlingen na te laten denken over hun eigen privacy: welke gegevens delen zijn met anderen met welke (mogelijke) gevolgen?
Het mediaprotocol dient in begrijpelijke en aansprekende taal is geschreven te zijn. Naast (of in) een mediaprotocol, maken scholen ook gebruik van een set regels die voorschrijven hoe leerlingen zich op internet moeten gedragen. Specifiek gaat het daarbij om het gebruik en netwerk van de school. Een set met losse afspraken over internet, wordt meestal een internetprotocol genoemd.

9.2 Gedragsregels voor medewerkers

Ook voor medewerkers is belangrijk om te weten hoe zij om moeten te gaan met Facebook, WhatsApp, Twitter en andere vormen van communicatie met leerlingen. De school hecht er waarde aan dat medewerkers de juiste keuze maken en daarom zijn er afspraken en gedragsregels. De afspraken en gedragsregels moeten voor alle leerlingen en medewerkers helder en toegankelijk zijn, zodat iedereen weet waar hij aan toe is.

9.3 Gebruik door de school

Sociale media worden ook door school zelf gebruikt. Het gebruik van sociale media kent een aantal risico's.

Facebook
Het is scholen toegestaan om een of meerdere accounts te hebben bij Facebook. De school mag enkel over een afgesloten account beschikken. Publieke accounts waarbij iedere willekeurige bezoeker de schoolinformatie kan zien, zijn niet toegestaan. Iedere gebruiker (bij Facebook "Vrienden"), moet geautoriseerd worden door de beheerder van het Facebookaccount.

Het gebruik van Twitter is toegestaan. Twitter is echter een open applicatie. Er wordt alleen gewerkt met volgen of niet volgen. In de zoekfunctie is echter altijd een bericht van een gebruiker terug te vinden. De beheerder controleert of iedere volger relevant is voor de school (ouder, betrokken bij school).
Items die op sociale media geplaatst mogen worden:

- Aankondigingen van gebeurtenissen of organisatie (Bijvoorbeeld: "Op 6 december is het studiedag voor alle leerkrachten. De kinderen zijn dan de hele dag vrij")
- Publiceren van recente activiteiten op school. (Bijvoorbeeld: bezoek van Sinterklaas aan school)
- Link naar de nieuwsbrief of item op website.
- Suggestieve foto's worden nooit geplaatst.

Bij alle publicaties wordt -zo nodig- slechts één foto gepubliceerd en wordt verwezen naar de website.

Op de website van de school en op Facebook/Twitter worden (indien van toepassing) foto's van activiteiten geplaatst die op school of namens school hebben plaatsgehad. Hierbij worden de volgende regels in acht genomen:

- Er wordt nooit een foto geplaatst waar een leerling alleen en frontaal op staat (portretfoto).
- Er wordt hoogstens een foto geplaatst waar kinderen "en profile" opstaan of in groepjes.
- Er worden geen foto's geplaatst waarvan de ouders van het kind geen toestemming hebben verleend voor plaatsing.
- Suggestieve foto's worden nooit geplaatst.
- Er worden geen meerdere foto's in een collage geplaatst.
- Foto's van gymmende kleuters in de speelzaal worden niet geplaatst.
- Foto's van andere sportende kinderen worden met terughoudendheid geplaatst.
- Er worden geen persoonlijke gegevens vermeld.

Iedere school van de SNB neemt in overleg met de MR een besluit over het wel of niet inzetten van Sociale Media. De inzet van Sociale Media gebeurt binnen de kaders van dit document.

Een Model reglement internet en sociale media op school met toelichting is toegevoegd als Bijlage 5.

10. Privacy bij overstapdossiers

Om de uitwisseling van leerling gegevens tussen scholen een wettelijke grondslag te geven, is er in 2012 een speciale wetswijziging (Wetsvoorstel 32.176 d.d. 8 maart 2012) doorgevoerd. Deze wet wijzigde verschillende andere onderwijswetten. Gelijktijdig met de wetswijziging is in het bijbehorende "*Besluit uitwisseling leer- en begeleidingsgegevens*" een beknopte opsomming gegeven welke gegevens scholen mogen uitwisselen.
In de wet is het belangrijkste uitgangspunt dat scholen altijd vooraf aan de uitwisseling moeten afwegen welke specifieke gegevens van iedere leerling daadwerkelijk nodig zijn ten behoeve van het leren en begeleiden van een leerling op de nieuwe school. Gegevens die niet aan dit criterium voldoen, mogen niet door scholen uitgewisseld worden (hoe handig het doorgeven van die informatie ook lijkt). De Minister van OCW noemt in de toelichting bij het Besluit het voorbeeld dat in geval van een goed functionerende leerling, de set van leer- en begeleidingsgegevens die uitgewisseld wordt, dus zeer summier zal kunnen zijn.
Met deze strikte regels en de beperkte set gegevens die volgens het Besluit mogen worden uitgewisseld, wil de Minister van OCW een belangrijke basisvoorwaarde geven voor een transparante elektronische uitwisseling van gegevens tussen scholen, waarbij de kans op fouten zo klein mogelijk is en de privacy van de betrokkenen gewaarborgd is.
De gewijzigde wetgeving biedt ruimte voor verschillende vormen van elektronische uitwisseling van gegevens tussen scholen. In het Besluit wordt letterlijk gesproken over een landelijke standaard en deze Overstapservice Onderwijs (voorheen bekend als Elektronisch Leerdossier of ELD).
Ook op het bewerken en uitwisselen van leerlinggegevens, is de Wet bescherming persoonsgegevens (Wbp) van toepassing. Er moet sprake zijn van een zogenoemde 'doelbinding' bij de vastlegging en bewerking van gegevens. Dit wil zeggen dat er alleen informatie mag worden opgeslagen, gebruikt en gedeeld als dit een specifiek en rechtmatig doel dient. Scholen mogen volgens artikel 11 van de Wbp alleen deze gegevens verwerken voor zover zij toereikend, ter zake dienend en niet bovenmatig zijn. Dit betekent dat er per leerling die overstapt, moet worden bepaald welke gegevens relevant en proportioneel zijn.

Daarnaast zijn de onderwijswetten van toepassing. In artikel 42 van de Wet op het primair onderwijs is vastgesteld dat een po-school verplicht is om een onderwijskundig rapport op te stellen en te verstrekken aan de nieuwe school. Daarnaast moet op grond van dat artikel een afschrift beschikbaar worden gesteld aan de ouders of verzorgers van de leerling. De po-school is verplicht om inzage in het dossier te verlenen aan de ouder. Voor verstrekking van het dossier aan vo-scholen is toestemming van de ouders/verzorgers verplicht.
De Inspectie van het Onderwijs zal toezicht houden op de juiste wijze van gegevensuitwisseling en naleving van de wettelijke bepalingen.

11. Stagiaires

Stagiaires hebben geen toegang tot bronnen die vertrouwelijke informatie bevatten. Toch kan het voorkomen dat een stagiaire met vertrouwelijke informatie in aanraking komt. De school spreekt met de stagiaire een geheimhoudingsovereenkomst af waarin beschreven staat dat de stagiaire tijdens en na de stage niet toegestaan is vertrouwelijke en privacygevoelige informatie met anderen te delen.

Een voorbeeld Geheimhoudingsovereenkomst is toegevoegd als bijlage 7

12. Transparantie

Scholen verzamelen en gebruiken persoonsgegevens van en over leerlingen. De school moet kunnen verantwoorden wat er met die gegevens gebeurt. De ouders, en leerlingen wanneer zij 16 jaar of ouder zijn, moeten daarom volstrekt helder, actief en begrijpelijk worden geïnformeerd. Welke persoonsgegevens worden er verzameld? En wat gebeurt er met de gegevens? Openheid en transparantie over de gegevensverwerking is een wettelijk uitgangspunt.

12.1 De school is transparant over:

- Het privacybeleid van de school in het algemeen (bijvoorbeeld het privacyreglement en/of mediaprotocol). In het inschrijfformulier voor nieuwe leerlingen wordt hierop al gewezen. Deze informatie wordt (ook) in de schoolgids en/of website opgenomen.
- Concrete uitwisselingen van gegevens met derden, zoals leveranciers van digitaal leermateriaal of leveranciers van leerlinginformatiesystemen.

12.2 Ouders actief informeren

De school is verplicht om ouders, en leerlingen wanneer zij 16 jaar of ouder zijn actief (ongevraagd) te informeren over de afspraken met de leveranciers. Deze (wettelijke) verplichting is ook opgenomen in het convenant ‘Digitale Onderwijsmiddelen en Privacy — Leermiddelen en Toetsen’. Een onderwijsinstelling moet ouders onder meer laten weten welke leveranciers de persoonsgegevens van hun kind ontvangen. Ook moet de school uitleggen (en kunnen garanderen) dat er goede afspraken zijn gemaakt (bijvoorbeeld door te verwijzen naar de bewerkersovereenkomsten).
Bij de verstrekking van adequate informatie aan de ouders, kunnen scholen gebruikmaken van de privacybijsluiter (bijlage in de bewerkersovereenkomst). Alle leveranciers die het convenant onderschrijven, zijn verplicht zo’n privacybijsluiter te verstrekken. In de bijsluiter wordt onder meer aangegeven welke persoonsgegevens worden verwerkt, welke andere partijen (‘onderaannemers’) de leverancier heeft ingeschakeld én waar de gegevens zijn opgeslagen.
Op de website enkel vertellen dat ‘de privacy goed is geregeld’, is niet voldoende. Een school is pas echt transparant als naast het privacyreglement, óók de privacybijsluiters (of een eigen uitleg) van de producten die de school gebruikt op bijvoorbeeld de website plaatst.

12.3 Bedenkingen over transparantie

Uit gesprekken met docenten en bestuurders blijkt dat scholen soms huiverig zijn om transparant te zijn: informatie geven aan ouders geeft hen misschien wel aanleiding om extra (lastige) vragen te stellen. In de praktijk lijkt dit gelukkig mee te vallen. Een school hoeft zich natuurlijk geen zorgen te maken als ze aan de wet voldoet: daar kunnen ouders niet tegen zijn. En daar komt bij dat de ervaring is dat ouders tegenwoordig mondiger zijn en ook zonder die transparantie kritische vragen stellen. En waarom zou een school de ouders een extra vraag in handen spelen door níet volledige transparantie te geven, zoals de wet dat van scholen vraagt?

Een aantal voorbeeldteksten transparantie over privacy is toegevoegd als Bijlage 6.

13. Conclusie

De Wet bescherming persoonsgegevens verplicht de SNB en haar scholen tot het nemen van een aantal stappen. Het aannemen van een privacyreglement is daar een belangrijk onderdeel van. De scholen zullen ieder met de leveranciers van hun applicaties afspraken moeten maken met een bewerkersovereenkomst om de privacy van de leerlingen en het personeel te waarborgen. Gelukkig zijn er veel hulpmiddelen beschikbaar om dit redelijk vlot te kunnen afwikkelen.
Als SNB bieden we onze leerlingen en personeel een goed beveiligd netwerk met veel mogelijkheden. Het is wel van belang dat met name personeel zich bewust is van de onveilige situaties die kunnen ontstaan door onzorgvuldig of nonchalant handelen. Technisch kunnen we hier ook maatregelen op nemen.
Bewustwording bij kinderen is van groot belang. Naast het leren omgaan met netwerk- en internetapplicaties, is het voor kinderen belangrijk om te weten wat er met hun privacy gebeurt als ze daarin niet zorgvuldig zijn. Dit dient ook aan bod te komen in de lessen mediawijsheid.
Gebruik maken van foto's van kinderen mag alleen na toestemming van de ouders. Hier is geen tussenweg in mogelijk.
Gebruik van sociale media is te begrijpen, maar een protocol is onmisbaar. De risico's bij sociale media zijn groter omdat hier de algemene voorwaarden van de applicaties van toepassing zijn. Heel vaak zijn die erg ongunstig voor het privacyrecht van de Nederlandse gebruiker.
Het is van belang om transparant te zijn over het privacybeleid van de instelling. Sterker nog: de wet schrijft dit voor.

14. Acties:

Fase 1

1. Beleidsstuk Privacy: Aanbieden aan bestuur en (G)MR om vast te stellen als beleid.

Fase 2a

1. Bewerkersovereenkomsten: aanbieden aan leveranciers (door iedere school afzonderlijk)
2. Aanpassingen op het netwerk:
   --wachtwoordbeleid
   --systeem automatisch op slot zetten
   --Invoeren e-maildisclaimer

Fase 2b

1. Vaststellen fotobeleid naar aanleiding van de Wbp door ieder school
2. Vaststellen Internet- of socialemediaprotocol door iedere school
3. Transparant communiceren naar ouders over privacybeleid van de scholen

Fase 3

1. Beleidsstuk Privacy: Evaluatie door MR's en MT's van de scholen aan het eind van schooljaar 2017-2018.
2. Evaluatie wordt gerapporteerd aan GMR en bestuur van de SNB.

15. Bronnen

- http://www.privacyconvenant.nl/het-convenant/
- Kennisnet: Privacy in 10 stappen
- https://www.kennisnet.nl/organiseren-ict/privacy/
- http://maken.wikiwijs.nl/60600/Privacyscan_voor_scholen
- Handboek OSO
- http://doorbraakonderwijsenict.nl/
- Like to Share (studiedag privacy & Big Data)
- APS IT Diensten (privacyworkshop - IPON)

Kees van der Plas
Beleidsmedewerker ICT
k.vdplas@nutsscholenbreda.nl
Maart 2016