Onderwijsstichting Wijzer aan de Amstel

Informatiebeveiligings- en privacy beleid

Vastgesteld door:

Vastgesteld op: 02-07-2019	Instemming GMR op: 02-07-2019
Eigenaar: M. Domela Nieuwenhuis Directeur-bestuurder	R. Bosboom Voorzitter

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 scholen worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard.

- Er komen steeds meer hacks en datalakken in het onderwijs voor
- Iedereen is wettelijk verplicht verantwoord met (persoons)gegevens om te gaan
- We maken steeds meer gebruik van ict en gepersonaliseerd leren, waardoor risico's ook toenemen

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 leiden tot inbreuken op het geven van onderwijs en het vertrouwen in onze scholen.

Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's die gepaard gaan met deze bedreigingen tot een zo beperkt mogelijk niveau te reduceren, zo niet te voorkomen. 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.

1.1.1 Informatiebeveiliging en privacy

Informatiebeveiliging is een proces voor het beschermen van de organisatie tegen risico's en bedreigingen met betrekking tot informatie en ict. Het richt zicht 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 integraal onderdeel van privacy.

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

2 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 privacyincidenten en de eventuele gevolgen hiervan worden voorkomen.

Dit beleid is een leidraad voor iedereen die betrokken is bij IBP binnen onze scholen. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen binnen Wijzer aan de Amstel. Het is van toepassing op de hele organisatie, waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.

Het informatiebeveiligings- en privacybeleid 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;

Dit beleid maakt duidelijk waar de verantwoordelijkheden rondom informatiebeveiliging en privacy zijn belegd.

3 Uitgangspunten

De belangrijkste beleidsuitgangspunten bij Wijzer aan de Amstel zijn:

- Informatiebeveiliging en de privacy dient te voldoen aan alle relevante wet- en regelgeving.
- Veilig en betrouwbaar omgaan met informatie is de verantwoordelijkheid van iedereen.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich ‘fatsoenlijk’ gedragen met een eigen verantwoordelijkheid.
- Als stichting / school zijn we eigenaar van de informatie die onder onze verantwoordelijkheid wordt gebruikt.
- We maken 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 informatiebeveiliging en privacy aan de ene kant en flexibiliteit/werkbaarheid aan de andere.

3.1.1 Privacy

We hanteren vijf vuistregels voor privacy:

1. Doelbepaling en doelbinding: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. 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.

4 Wet- en regelgeving

Wijzer aan de Amstel voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht
- De bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 2.0'.leidend bij het maken van afspraken met leveranciers.
-

5 Organisatie

Dit hoofdstuk beschrijft hoe IBP is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

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

5.1.1 Richtinggevend

Eindverantwoordelijke

Het bevoegd gezag 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 management rapportages geëvalueerd.

5.1.2 Sturend

Functionaris gegevensbescherming (FG)

Volgens artikel 39 van de AVG, vervult de FG ten minste de volgende taken:

1. Het bestuur, directie(s) en de werknemers die persoonsgegevens gebruiken, informeren en adviseren over hun verplichtingen ten aanzien de wettelijke vereiste bescherming van persoonsgegevens.

2. Toezien op naleving van de:
   a. AVG,
   b. andere Unierechtelijke (lees: Europese) of nationale gegevensbeschermingsbepalingen, en
   c. van het beleid van het bestuur met betrekking tot de bescherming van persoonsgegevens (inclusief van verantwoordelijkheden, bewustmaking en opleiding van de medewerkers, en de betreffende audits.

De AVG spreekt er over dat de FG het bestuur 'bijstaat bij het toezicht op de interne naleving van de AVG'.

3. Gevraagd en ongevraagd advies geven met betrekking tot de gegevensbeschermingseffect-beoordeling (data protection impact assessments; DPIA) en toezien op de uitvoering daarvan in overeenstemming met de AVG. Om dit goed uit te voeren, kunnen FG's onder andere:

   a. informatie verzamelen om het (type) gebruik van persoonsgegevens te identificeren;
   b. analyseren en controleren in hoeverre het gebruik van persoonsgegevens aan de AVG voldoet; en
   c. het bestuur informeren, adviseren of aanbevelingen geven.

4. Met de Autoriteit Persoonsgegevens (AP) samenwerken en voor de AP optreden als contactpunt inzake met verwerking van persoonsgegevens verband houdende aangelegenheden, en – waar passend - overleg plegen over enige andere aangelegenheid aangaande privacy.

5. De FG is verplicht bij de uitvoering van zijn taken rekening te houden met de aan het gebruik van persoonsgegevens verbonden risico's, en met de aard, de omvang, de context en de doelen van het gebruik van die gegevens.

Directeur (domeinverantwoordelijkheid/proceseigenaar)

Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel, administratie et cetera. De directeur van de school is verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies. De directeuren stemmen deze richtlijnen, procedures en instructies af met de directeuren van de stichtingen.

5.1.3 Uitvoerend

Systeembeheerder

De systeembeheerder vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging.

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden.

Medewerkers hebben de plicht actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van beveiligingslekken, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).

Directeur

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere directeur 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 beleidsmedewerker IBP.

6 Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar geëvalueerd in het Directeurenoverleg en waar nodig bijgesteld door de Functionaris gegevensbescherming.

6.1.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Het Directeur-bestuurder, de Functionaris gegevensbescherming en de directeuren dragen zorg voor het voortdurend aanscherpen van het bewustzijn van de individuele medewerkers, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

6.1.2 Risico en beveiliging

Bij informatievoorziening zijn beschikbaarheid, integriteit en vertrouwelijkheid van groot belang. Het beveiligen van informatie is daarbij noodzakelijk van groot belang. Welke risico's zien we in het kader van IBP? Welke beveiligingsmaatregelen moeten worden genomen? De directeuren hebben hier voortdurend aandacht voor.

6.1.3 Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij het bestuurskantoor. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

6.1.4 Naleving

De naleving bestaat uit toezicht door de directeur op de dagelijkse praktijk van het IBP proces. Iedere medewerker neemt zijn verantwoordelijkheid. Directeuren spreken medewerkers aan in geval van tekortkomingen. Er wordt in teamvergaderingen aandacht besteed aan IBP.

Zie bijlage 2: Protocol melding beveiligingsincidenten en datalekken

Bijlage 1: Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Directeur-bestuurder Directeur	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Basismaatregelen opstellen • Privacyreglement vaststellen
Sturend (tactisch)	Functionaris gegevensbescherming	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert Directeurbestuurder/directie over IBP • Voorbereiden uitvoeren IBP-beleid • 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 • Afwikkeling klachten en incidenten	Processen, richtlijnen en procedures IBP, waaronder: • Protocol beveiligingsincidenten en datalekken • Bewerkersovereenkomsten regelen • Brief toestemming gebruik foto's en video • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Bewustwording: activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leer-lingen
	Directeur domeinverantwoordelijke / proceseigenaar Domeinen: ict, personeel, facilitair, onderwijs, financiën, inkoop en administratie	• Toegangsbeleid zowel fysiek als digitaal vaststellen. • Samen met systeembeheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met systeembeheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) Bepalen op welke wijze IBP wordt vormgegeven in richtlijnen, procedures, protocollen en instructies en dir afstemmen met de collega directeuren.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Uitvoerend (operationeel)	Systeembeheerder	• Technisch aanspreekpunt voor IBP incidenten.	
	Medewerker	• Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	Meldingen doorgeven aan de directeur.
	Directeur	• Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur. • Incidentafhandeling (registreren en evalueren).	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

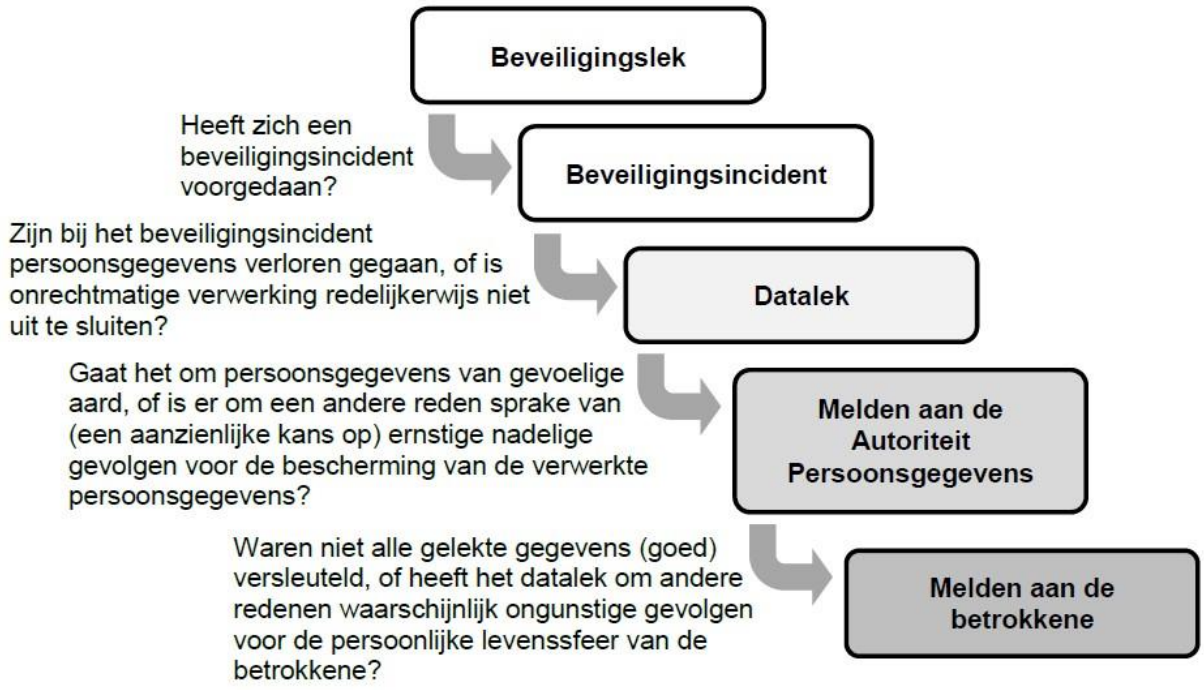
Bijlage 2: Protocol melding informatiebeveiligingsincidenten en datalekken

Organisaties die persoonsgegevens verwerken, dus ook scholen, zijn verplicht om binnen 72 uur hiervan een melding te maken bij de Autoriteit Persoonsgegevens (AP) wanneer er sprake is van een datalek.

Een datalek is “een inbreuk in de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens”.
Persoonsgegevens betreffen alle informatie over een natuurlijk persoon (lees: leerling, ouder, medewerker).

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is het bestuur.
Een softwareleverancier is een bewerker voor de school. Er kan worden afgesproken dat een bewerker namens de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het bestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

Beslisboom: wanneer moet je een melding maken en waar?



1. Er is alleen sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van persoonsgegevens niet uitgesloten kunnen worden.
2. Als het datalek ook nadelige gevolgen kan hebben voor de persoonlijke levenssfeer van de betrokken personen, dan dienen zij ook op de hoogte gesteld te worden van het datalek.

Als er alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. Er hoeft dan geen melding gedaan te worden bij de Autoriteit Persoonsgegevens.

Meldingen bij de AP kunnen gedaan worden via het online meldloket dat hier te vinden is.
https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Info:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf

Het nalaten van deze melding kan leiden tot een fikse boete.

Procedure

1. Ontdekken
   De ontdekker merkt een beveiligingsincident op en verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het de directeur die de melding bespreekt met de functionaris gegevensbescherming. (FG = functionaris, die hiervoor namens het bestuur is aangewezen).

2. Inventariseren
   Samen wordt bepaald of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan worden aanvullende vragen gesteld aan de ontdekker en/of de systeembeheerder / ICT'er. De volgende informatie wordt daarna vastgelegd:
   - Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
   - Datum/periode van het beveiligingsincident
   - Aard van het beveiligingsincident
   - Wanneer van toepassing (bij een datalek):
     - Omschrijving van de groep betrokkenen o Aantal betrokkenen o Type persoonsgegevens in kwestie
     - Worden de gegevens binnen een keten gedeeld

3. Beoordelen (zie beslisboom)
   Wanneer voldoende informatie is verzameld, en er een datalek wordt vermoed, worden de feiten beoordeeld om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is. Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', houd je rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er gemeld worden.
   Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens "gevoelig" zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

   De volgende informatie wordt vastgelegd door de FG:

   - Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen • Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
   - Wordt het datalek aan betrokkenen gemeld? Waarom niet?
   - Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

4. Repareren
   De systeembeheerder / ICT'er wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. Hij/zij legt onderstaande vast:

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.

- Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

5. Melden
   Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de FG dit binnen 72 uur doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0. Bekijk ook daar om te zien welke informatie er eigenlijk nodig is om een datalek te melden.

6. Vastleggen
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident is afgesloten.

7. Informeren betrokkene: leerling en/of zijn ouders
   Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, of ouders. In principe kan er van worden uitgaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Bijlage 3: Afspraken over foto’s en video - toestemming

De wetgever gaat er van uit dat je vooraf toestemming vraagt voor het gebruik van foto’s van leerlingen. Zonder die toestemming mag je geen foto’s en video’s van leerlingen gebruiken. En wil je toestemming vragen, hou dan rekening met twee belangrijke punten:

- Ouders/verzorgers moeten expliciet kunnen aangeven waar ze wel of geen toestemming voor verlenen. De keuze moet duidelijk aan te geven zijn, bijvoorbeeld door een kruisje in een vakje te zetten bij bepaalde type media (foto's/film) of bij bepaalde uitingen (website, schoolkrant, etc.).
- Zorg voor gelaagde toestemming: wil je toestemming voor foto’s op de website, in de schoolgids, nieuwsbrief of in sociale media?

Zorg dat je als school vooraf de juiste afspraken hebt gemaakt en dat iedereen ook weet wat die afspraken zijn.

1. Vraag uitdrukkelijk toestemming
Een foto waarop een leerling herkenbaar in beeld is, zegt iets over de leerling. Die foto is een persoonsgegeven. Wil de school een foto van een leerling op de schoolwebsite zetten? De privacywetgeving eist dat daar vooraf uitdrukkelijk toestemming voor wordt gevraagd.

2. Kom elk jaar terug op de afspraak
Meestal wordt de toestemming geregeld bij de inschrijving van de leerling. Maar het is de bedoeling dat de school jaarlijks terugkomt op de gemaakte afspraak. Het is noodzakelijk bij het begin van het schooljaar even aandacht te besteden aan de gemaakte keuze van de ouders. Dat kan eenvoudig in een brief of nieuwsbrief ('wilt u uw toestemming intrekken, loop dan even langs bij …').

3. Geef ouders toegang tot de foto's
Het kan een hele uitdaging zijn voor scholen om ieder jaar toestemming te vragen aan ouders. Met de nieuwe Europese privacywet is daar vanaf mei 2018 geen ontkomen meer aan. Het regelen van toestemming kan ook praktisch worden aangepakt. Geef ouders bijvoorbeeld toegang tot de foto's, zodat zij weten welke foto's er worden gemaakt en gebruikt.
Advies: beveilig de foto's op de schoolwebsite en geef ouders toegang met een wachtwoord. Het is handig om die toegang - bijvoorbeeld - tegelijk te regelen met een account voor de digitale nieuwsbrief.

4. Van Facebook tot folder: vraag specifiek toestemming
Ouders moeten weten waar ze toestemming voor geven als de school foto's wil gebruiken. Dat moet bij het toestemmingsformulier worden verteld. Bij sociale media is het verstandig apart toestemming te vragen voor het gebruik van een foto. Een foto op Facebook of Twitter wordt niet meer op de site van school, maar - in dit geval - in Amerika opgeslagen.
Ook voor een folder, kalender of schoolgids kan het beste apart toestemming worden gevraagd. Vooraf regelen kan vragen achteraf voorkomen. Vraag dus niet ieder jaar om algemene toestemming ('ja, ik geef toestemming om foto's van mijn kind op de site van de school te zetten'), maar vraag specifieke toestemming ('ja, ik geef toestemming voor 1. de website ja/nee, 2. sociale media ja/nee, 3. de schoolgids ja/nee, 4. de nieuwsbrief ja/nee).

5. Geen toestemming is geen publicatie
Als ouders geen toestemming hebben gegeven voor gebruik van foto's, dan zorgt de school er natuurlijk voor dat de foto's niet op internet verschijnen.

Voorbeeldbrief “Toestemming publicatie foto’s en video’s: zie hierna.

[Plaats], [maand] [jaar]

Beste ouder/verzorger,

Op onze school laten wij u met foto’s en video’s zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Bijvoorbeeld tijdens activiteiten, schoolreisjes en lessen. Ook uw zoon/dochter kan op deze foto’s (en soms in video’s) te zien zijn.

Natuurlijk gaan we zorgvuldig om met foto’s en video’s. Wij plaatsen geen foto’s waardoor leerlingen schade kunnen ondervinden. We plaatsen bij foto’s en video’s geen namen van leerlingen. Toch vinden we het belangrijk om uw toestemming te vragen voor het gebruik van foto’s en video’s van uw zoon/dochter. Het is goed mogelijk dat u niet wilt dat foto’s van uw kind op internet verschijnen.

Met deze brief vragen we daarom uw toestemming voor het gebruik van beeldmateriaal van uw zoon/dochter. Wilt uw deze brief of antwoordstrook met uw kind meegeven naar school?

Uw toestemming geldt alleen voor foto’s en video’s die door ons, of in onze opdracht worden gemaakt. Het kan voorkomen dat andere ouders foto’s maken tijdens schoolactiviteiten. De school heeft daar geen invloed op, maar wij gaan ervan uit dat deze ouders ook terughoudend zijn bij het plaatsen van foto’s en video’s op internet.

Wilt u uw toestemming samen met uw zoon/dochter bespreken? We merken dat oudere leerlingen soms zelf een keuze willen maken om foto’s te gebruiken. Als u uw keuze thuis bespreekt, dan weten ze zelf waarom het gebruik van foto’s en video’s wel of niet mag.

Als we foto’s en video’s willen laten maken voor onderzoeksdoeleinden, bijvoorbeeld om een les van de leerkracht op te nemen, zullen we u daar apart over informeren en zo nodig om toestemming vragen. Ook als we beeldmateriaal voor een ander doel willen gebruiken, nemen we contact met u op.

U mag natuurlijk altijd terugkomen op de door u gegeven toestemming. Ook mag u op een later moment alsnog toestemming geven.

Alvast bedankt voor uw medewerking!

Met vriendelijke groet,

[naam ondertekenaar]

Hierbij verklaart ondergetekende, ouders/verzorger van …….. groep ……..

dat foto’s en video’s door school gebruikt mogen worden*:

□ in de schoolgids en schoolbrochure en schoolkalender
□ op de website van de school
□ in de (digitale) nieuwsbrief
□ op sociale-media accounts van de school (Twitter, Facebook)

* aankruisen waarvoor u toestemming geeft

Datum: .....

Naam ouder/verzorger: .....

Handtekening ouder/verzorger: .....

Toelichting gebruik formulier toestemming

Er is geen toestemming van ouders nodig voor het gebruik van foto's en video's in de klas en les voor onderwijskundige doeleinden. Ook is er geen toestemming nodig voor het plaatsen van een foto op een schoolpas of voor gebruik van een foto in het administratiesysteem. Wel gelden voor het gebruik van dat beeldmateriaal de gewone privacyregels (zoals dataminimalisatie: terughoudend omgaan met foto's en video's van leerlingen).

In het toestemmingsformulier is aparte toestemming opgenomen voor verschillende categorieën. De wetgever eist dat een ouder een goedgeïnformeerde beslissing kan nemen, die ook specifiek is. Het vragen van toestemming 'voor gebruik van foto's door de school' is dat zeker niet. Als school mag je je het dus niet zo formuleren: 'als u niet wilt dat we foto's van uw kind gebruiken, moet u dat maar zeggen'. Dit is een 'opt-out', en dit is in strijd met de wet.

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. 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 personeel van de school.

Toestemming geven door één of twee ouders
Het is de vraag of de toestemmingsverklaring door één of beide ouders moeten worden ondertekend.

Als leerlingen jonger zijn dan 16 beslissen de wettelijk vertegenwoordigers (de ouders) over de privacy. De wet gaat ervan uit dat je als school mag vertrouwen op de mededelingen van één ouder. Als dat vertrouwen terecht is, dan is de andere ouder ook gebonden aan die mededeling. Bij het ondertekenen van de toestemmingsverklaring, mag de school dus vertrouwen op de toestemming als één ouder die geeft. Alleen als de school weet dat de andere ouder (die niet getekend heeft) tegen de toestemming is, mag de school niet uitgaan van die ene ondertekening. Dan moet de school van beide ouders toestemming hebben. Vooral bij gescheiden ouders kan het verstandig zijn om de toestemming van beide ouders te vragen. Voor het intrekken van toestemming is de mededeling van één ouder ook voldoende.

Bij twijfel is het beter om te vertrouwen op twee handtekeningen, of om de foto dan maar niet te gebruiken.

Bijlage 4: Schoolgids en IBP – voorbeeld teksten om ouders te informeren

Op school wordt zorgvuldig omgegaan met de privacy van onze leerlingen. Op onze administratie is de Wet bescherming persoonsgegevens van toepassing. Dit betekent onder andere dat de gegevens door ons worden beveiligd, en dat de toegang tot de administratie is beperkt tot alleen personeel die de gegevens strikt noodzakelijk nodig heeft. U heeft als ouder het recht om de door ons geregistreerde gegevens in te zien (voor zover die informatie betrekking heeft op uw kind). Als de gegevens niet kloppen, dan mag u van ons verwachten dat wij – op uw verzoek - de informatie verbeteren of aanvullen.

In verband met het geven van onderwijs, het begeleiden van onze leerlingen, en de vastlegging daarvan in de administratie van de school, worden er gegevens over en van leerlingen vastgelegd. Deze gegevens worden persoonsgegevens genoemd. Het vastleggen en gebruik van deze persoonsgegevens is beperkt tot informatie die strikt noodzakelijk is voor het onderwijs. De gegevens worden beveiligd opgeslagen en de toegang daartoe is beperkt.

De school maakt ook gebruik van digitaal leermateriaal. De leveranciers van die leermaterialen ontvangen een beperkt aantal leerlinggegevens. De school heeft haar leveranciers strikte afspraken gemaakt (bewerkersovereenkomst) over het gebruik van persoonsgegevens, zodat misbruik wordt voorkomen.
Als u hierover meer wilt weten kunt u kijken op: http://www.privacyconvenant.nl/de-deelnemers/

Leerlinginformatie wordt alleen gedeeld met andere organisaties als ouders daar toestemming voor geven, tenzij die uitwisseling verplicht is volgens de wet.

Om leerlingen eenvoudig toegang te geven tot digitaal leermateriaal van de school, maakt onze school gebruik van bijvoorbeeld Basispoort. Deze software maakt het geven van onderwijs op maat via gedigitaliseerde leermiddelen mogelijk. Het maken van bijvoorbeeld een online toets is alleen mogelijk als de docent weet welke leerling de antwoorden heeft ingevoerd. Hiervoor zijn leerlinggegevens nodig. De school heeft met Basispoort een overeenkomst gesloten waarin afspraken zijn gemaakt over het gebruik van de leerlinggegevens. Basispoort maakt gebruik van de volgende set met gegevens: een identificatienummer van Basispoort, voornaam, achternaam, tussenvoegsel, geboortedatum, leerlingkey, groepskey, groepsnaam, jaargroep, geslacht en het identificatienummer van de school. Via Basispoort worden er dus geen leer- of toetsresultaten opgeslagen en/of uitgewisseld.

Op onze school wordt er, per klas, een klassenlijst gemaakt met de adressen van leerlingen. Deze lijst met contactgegevens is erg praktisch om te overleggen met andere ouders, als de kinderen (buiten schooltijd) willen afspreken of als er vragen zijn rondom school, overblijf of bijvoorbeeld huiswerk. Wij vragen hierbij uw toestemming om de naam van uw kind, diens adres en uw telefoonnummer te mogen delen met de andere (ouders van de) klasgenootjes van uw kind. Als u er bezwaar tegen heeft, wordt de naam van uw kind niet gedeeld (en moet u daar zelf voor zorgen). Deze informatie op de klassenlijst mag uitsluitend gebruikt worden voor persoonlijk gebruik onderling, en dus niet voor bijvoorbeeld reclame.

Hierbij maak ik, wel / geen * bezwaar tegen het in de klas van mijn kind verspreiden van een klassenlijst met de naam van mijn kind, adres en telefoonnummer.

* doorhalen wat niet van toepassing is.

Bijlage 5: Privacyreglement m.b.t. IBP Beleid

1. Aanhef	Dit reglement is voor de scholen die vallen onder de stichting Wijzer aan de Amstel.	Iedere medewerker dient kennis te nemen van dit reglement en het beleid m.b.t. IBP
2. Definities Persoonsgegevens	Elk gegeven betreffende een natuurlijke persoon;	Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen.
Verwerking van persoonsgegevens	Eke 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;	Alles wat je met persoonsgegevens doet zoals: verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorsturen, beschikbaar maken, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen.
Bijzondere persoonsgegevens	Een persoonsgegeven dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid of zijn gezondheid;	
Betrokkene	De betrokkene is de leerling over wie de persoonsgegevens iets zeggen heeft;	
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;	Als de leerling nog geen 16 jaar is, dan beslissen zijn ouders over de privacy van de leerling.
Verantwoordelijke	De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Dat wil zeggen de rechtspersoon waar de school onder valt: het bevoegd gezag. Wanneer er in dit regelement gesproken wordt over de Verantwoordelijke dan wordt daarmee het bevoegd gezag van de school bedoeld.	De directeur geeft aan waarvoor en hoe de persoonsgegevens verwerk moeten worden. De schooldirecteur handelt de dagelijkse kwesties rondom privacy op school af, maar het bevoegd gezag blijft eindverantwoordelijk voor de verwerking van persoonsgegevens voor alle scholen die onder het bevoegd gezag vallen.

Bewerker	Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;	Het bedrijf, instelling of leverancier die in opdracht van de school de persoonsgegevens verwerkt.

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;	
School	De verantwoordelijke onderwijsinstelling / bevoegd gezag.	De verantwoordelijke school / het bevoegd gezag
3. Reikwijdte en doelstelling	1. Dit reglement stelt regels over de verwerking van persoonsgegevens van leerlingen van de school. 2. Dit reglement is van toepassing op alle persoonsgegevens van leerlingen die door de school 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; de rechten van betrokkene te waarborgen.	Dit reglement gaat over het gebruik van persoonsgegevens van leerlingen. Dit reglement geeft uitleg over het gebruik van persoonsgegevens en heeft tot doel bewustwording te creëren.
4. Doelen van de verwerking van persoonsgegevens	Bij de verwerking van persoonsgegevens houdt de school zich aan de relevante wetgeving waaronder de Wet bescherming persoonsgegevens.	

Doelen	Persoonsgegevens worden alleen gebruikt voor: a. de organisatie of het geven van het onderwijs, het begeleiden van leerlingen en het geven van studieadviezen; b. het aanbieden van leermiddelen; c. het bekend maken van informatie over de school, leermiddelen of leerlingen op de eigen website zolang dit gaat over het organiseren of geven van onderwijs of het geven van studieadviezen. d. het bekendmaken van schoolactiviteiten op de eigen website; e. de administratie van bijdragen of vergoedingen voor	

	leermiddelen en buitenschoolse activiteiten. f. het behandelen van geschillen en het laten uitvoeren van accountantscontrole; g. het onderhouden van contacten met oud-leerlingen van de school; h. 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.	De wet verplicht om het verwerken van persoonsgegevens aan te melden bij de toezichthouder College Bescherming Persoonsgegevens (CBP). Voor scholen is hiervoor een uitzondering gemaakt als de verwerking plaats vindt voor de doelen zoals die zijn omschreven in artikel 4. Als de school de persoonsgegevens voor een ander doel wil gaan gebruiken, dan moet dat doel worden toegevoegd aan artikel 4, én dan moet die verwerking apart worden aangemeld bij het CBP. In dat geval dient aan dit artikel worden toegevoegd: “Het bevoegd gezag heeft deze verwerking gemeld bij het CBP onder NUMMER”.

6. Doelbinding	Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. De school verwerkt niet meer gegevens dan noodzakelijk is om die vastgestelde doelen te bereiken.	Persoonsgegevens mogen alleen gebruikt worden om het gestelde doel te bereiken. Gegevens mogen dus wel worden gebruikt voor een nevendoel, maar dan moet dat wel samenhangen met de oorspronkelijke doeleinden waarvoor de gegevens verzameld zijn.
7. Soorten gegevens	De door de school gebruikte categorieën van persoonsgegevens worden in bijlage 1 opgesomd.	In bijlage 1 staan welke persoonsgegevens door school worden verwerkt om het gestelde doel te bereiken
8. Grondslag verwerking	Verwerking en gebruik van persoonsgegevens gebeurt alleen op grond van: A: Toestemming: er is toestemming verleend door betrokkenen of de wettelijk vertegenwoordiger B: Overeenkomst: in het geval de gegevensverwerking noodzakelijk is voor de uitvoering van een	
	overeenkomst waarbij de betrokkene partij is. C: Wettelijke verplichting: in het geval de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan het bevoegd gezag onderworpen is. D: Vitaal belang. E: Publiekrechtelijke taak: in het geval de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak: onderwijs geven F. Gerechtvaardigd belang:	
9. Bewaartermijnen	De school 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.	De school bewaart de gegevens niet langer dan dat ze nodig zijn om het doel te bereiken tenzij er een wettelijke bewaarplicht geldt.

10. Toegang	De school verleent slecht toegang tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan: A: de bewerker en de derde die onder rechtstreeks gezag van de school staat; B: de bewerker die gemachtigd is om persoonsgegevens te verwerken;' 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.	Alleen personen of bedrijven die onder rechtstreeks gezag van de school staan krijgen als dat nodig is toegang tot de gegevens
11. Beveiliging en geheimhouding	A: De school neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden gestolen, beschadigd, verloren gaan of onrechtmatig worden verwerkt/gebruikt. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. B: De school zorgt dat medewerkers niet meer inzage of toegang hebben tot de	De beveiliging voorkomt dat de gegevens door alle medewerkers voor allerlei andere doelen gebruikt ('misbruikt') kunnen worden. De school zorgt er voor dat de toegang tot de administratie en systemen beperkt is: niet alle medewerkers hoeven noodzakelijkerwijs inzage te hebben in de gehele administratie. De medewerkers zorgen ervoor dat onbevoegden op hun computer / laptop geen toegang kunnen krijgen tot

	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 school rekening met de concrete risico's die van toepassing kunnen zijn op de verwerkte persoonsgegevens. 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.	persoonsgegevens. Useridentificatie (gebruikersnaam) en authenticatie (bijvoorbeeld wachtwoord) zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven. Computer in de slaapstand als je er bij wegloopt en geen zicht hebt op eventuele onrechtmatige gebruikers. Uitschakelen aan het eind van de werkdag. De school zorgt dat de gegevens voldoende beveiligd zijn, en dat de beveiliging bijgewerkt blijft. Daarbij wordt ook rekening gehouden met de speciale beveiligingsrisico's die op de school van toepassing zijn (dat kunnen bijvoorbeeld beveiligingsincidenten uit het verleden zijn). Bij het meenemen van laptops of usb-sticks naar huis moet er aan gedacht worden of ze voldoende beveiligd zijn bij verlies. Voor iedereen die binnen de school de beschikking krijgt over persoonsgegevens, is verplicht die vertrouwelijk te behandelen. Voor medewerkers geldt meestal (al) een geheimhoudingsclausule die in de arbeidsovereenkomst is opgenomen.
12. Verstrekken gegevens aan derden	Wanneer daartoe een wettelijke plicht bestaat kan de school de persoonsgegevens verstrekken aan derden. Het verstrekken van persoonsgegevens aan derden kan ook plaatst vinden na toestemming van de betrokkene.	Als de wet dat verplicht kan de school de persoonsgegevens aan derden geven. Dit kan ook als de betrokkene aan school toestemming geeft om zijn persoonsgegevens aan een derde te geven.
13. Sociale media	Voor het gebruik van persoonsgegevens in sociale media, zijn ook afspraken gemaakt in het protocol sociale media. Werknemers mogen via sociale media geen vertrouwelijke en/of schadelijke informatie verstrekken over de schoolorganisatie en de betrokkenen bij de organisatie.	Er kan voor gekozen worden om hier één of meerdere bepalingen op te nemen over het gebruik van internet of sociale media. Het is ook mogelijk dit op te nemen in aparte gedragsregels of een protocol.
14. Rechten betrokkenen	1. De Wbp geeft de betrokkene een aantal rechten. De school erkent deze rechten en handelt in overeenstemming met deze rechten.	De school houdt zich bij het verwerken van persoonsgegevens aan alle van toepassing zijnde wet- en regelgeving, ook op het

		gebied van rechten van betrokkenen. De school kan vragen om een geldig identiteitsbewijs om de identiteit van de verzoeker vast te stellen.
Inzage	a. De wettelijk vertegenwoordiger van de leerling heeft recht op inzage van de door school verwerkte persoonsgegevens betreffende de leerling.	De school moet aan dit verzoek gehoord geven tenzij dat het niet mogelijk is het verzoek uit te voeren of wanneer het uitvoeren daarvan heel veel moeite zou kosten.
Verbetering, aanvulling, verwijdering en afscherming	b. De wettelijk vertegenwoordiger van de leerling kan een verzoek doen tot verbetering, aanvulling, verwijdering of afscherming van zijn persoonsgegevens, tenzij dit onmogelijk blijkt of een onredelijke inspanning zou vergen.	Als de school persoonsgegevens verwerkt, en daarvoor geen grondslag heeft in de wet, of geen toestemming heeft, dan kan de verzet worden ingesteld tegen het gebruik van die gegevens.
Verzet	c. Voor zover de school persoonsgegevens gebruikt op de grondslag van artikel 8 onder e en f, dan kan de wettelijk vertegenwoordiger van de leerling zich verzetten tegen verwerking van persoonsgegevens op basis van diens persoonlijke omstandigheden.	Binnen 4 weken na het indienen van een verzoek moet de school het verzoek uitvoeren of uitleggen waarom ze het verzoek niet (gaan) uitvoeren.
Termijn	2. De school dient binnen een termijn van 4 weken na ontvangst van een verzoek hieraan schriftelijk gehoor te geven dan wel deze schriftelijk, gemotiveerd af te wijzen. De school kan de betrokkene laten weten dat er meer tijd nodig en deze termijn verlengen met maximaal 4 weken.	Wanneer de school akkoord gaat met het verzoek dan doet zij dit zo snel mogelijk.
Uitvoeren verzoek	3. Indien het verzoek van de betrokkene wordt gehonoreerd, draagt de school zorg voor het zo spoedig mogelijk doorvoeren van de verzochte wijzigingen.	Als u toestemming heeft gegeven voor het gebruik van persoonsgegevens, dan kunt u dit op ieder moment weer intrekken.
Intrekken toestemming	4. Voor zover voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming ten allen tijden door de wettelijk vertegenwoordiger van de leerling worden ingetrokken.	

15. Transparantie	1. De school informeert de betrokkene over de verwerking van zijn persoonsgegevens. Indien	Wanneer de wet dat verplicht worden betrokkene geïnformeerd over het gebruik van hun
	het type verwerking dat vraagt, informeert de school iedere betrokkene apart over de details van die verwerking. 2. De school informeert de betrokkene – op hoofdlijnen – ook over de afspraken die gemaakt zijn met derden en bewerkers die persoonsgegevens van de betrokkene ontvangen.	persoonsgegevens. Dat kan via bijvoorbeeld de schoolgids of de website. Indien dat nodig is, dan worden de (ouders van de) leerlingen individueel geïnformeerd, bijvoorbeeld in het geval van verwerking van gezondheidsgegevens.
16. Klachten	1. Wanneer de wettelijk vertegenwoordiger van de leerling van mening is dat het doen of nalaten van de school niet in overeenstemming is met de Wbp of zoals dat is uitgewerkt in dit reglement is, dan dient hij/zij dit aan te geven bij de directeur van de school. 2. De klachtenprocedure van de stichting (schoolgids/website) dient te worden gevolgd.	
17. Onvoorziene situatie	Indien er zich een situatie voordoet die niet beschreven is in dit reglement dan neemt het bevoegd gezag de benodigde maatregelen.	Dit reglement voorziet niet in alle gevallen, wanneer er zoiets gebeurt dan is het aan het bevoegd gezag om daarover te beslissen.
18. Wijzigingen reglement	Dit reglement wordt na instemming van de (G)MR vastgesteld door het bevoegd gezag. De school maakt dit reglement openbaar via de website (schoolgids). Het bevoegd gezag heeft het recht dit reglement, na instemming van de (G)MR te wijzigingen.	Het reglement wordt openbaar gemaakt via bijvoorbeeld de website, schoolgids of wordt uitgereikt aan ouders die hun kind inschrijven.
19. Slotbepaling	Dit reglement wordt aangehaald als “het privacyreglement” en treedt in werking op 01-05-2018	

Bijlage 5: Privacyreglement m.b.t. IBP Beleid

BIJLAGE bij het privacyreglement: Overzicht van categorieën gebruikte persoonsgegevens

Omschrijving en opsomming categorieën Persoonsgegevens die gebruikt worden:

Bijvoorbeeld:

a. naam, voornamen, voorletters, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de betrokkene;
b. het persoonsgebonden nummer (BSN);
c. nationaliteit;
d. gegevens als bedoeld onder a, 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 school, 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. schoolgegevens (waaronder naam school, naam intern begeleider, klas/groep waarin de leerling zit, tijdstip van inschrijving bij deze school, naam van de indiener van de aanmelding bij het samenwerkingsverband, schoolloopbaan en rapportage vanuit primair naar het 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 school 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 ouderbijdrage; n.

Bijlage 6: Bewerkersovereenkomst

Het bevoegd gezag heeft afspraken gemaakt met softwareleveranciers op basis van de Model Bewerkersovereenkomst 2.0 behorende bij het Convenant Digitale Onderwijsmiddelen en Privacy 2.0

https://www.privacyconvenant.nl/

Deze Model Bewerkersovereenkomst bevat altijd twee bijlagen:
1. In de Privacy Bijsluiter wordt een beschrijving gegeven van de dienstverlening, producteigenschappen en welke categorieën Persoonsgegevens worden verwerkt en onder welke doeleinden deze verwerkingen vallen.
2. In de Technische en Organisatorische Maatregelen wordt omschreven welke beveiligingsmaatregelen er worden getroffen. De beveiliging dient een continu punt van aandacht en zorg te blijven.

Bijlage 7: Modelprotocol social media

Modelprotocol social media

Inleiding
Social media zijn een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Onder de noemer social media worden onder andere weblogs of blogs, social bookmarking, videosites als YouTube en sociale netwerken als Facebook geschaard. Via deze media delen mensen verhalen, beeldmateriaal, kennis en ervaringen.
Dit doen zij door berichten te publiceren of door gebruik te maken van reactiemogelijkheden.

Er is discussie over de vraag of WhatsApp, Instagram, Snapchat en vergelijkbare apps deel uitmaken van het begrip social media.
Omdat blijkt dat door ouders/verzorgers, leerlingen en vaak ook de leerkracht gebruikt gemaakt wordt van dergelijke apps, worden zij in dit protocol gezien als social media.

Social media bieden de mogelijkheid om te laten zien dat je trots bent op je school en kunnen een bijdrage leveren aan een positief imago van de scholen die resulteren onder Wijzer aan de Amstel. Van belang is te beseffen dat je met berichten op social media (onbewust) de goede naam van de school en betrokkenen ook kunt schaden. Om deze reden vragen wij om bewust met de social media om te gaan.

Essentieel is dat de onderwijsinstellingen en de gebruikers van social media tegenover alle betrokkenen de reguliere fatsoensnormen in acht blijven nemen en de nieuwe mogelijkheden met een positieve instelling benaderen.

De stichting Wijzer aan de Amstel vertrouwt erop dat haar medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen verantwoord om zullen gaan met social media en hebben dit protocol opgezet om een ieder die bij een van de stichtingen werkzaam of betrokken is, of zich daarbij betrokken voelt, daarvoor richtlijnen te geven.

Uitgangspunten

1. De stichting Wijzer aan de Amstel onderkent het belang van social media.
2. Dit protocol draagt bij aan een goed en veilig school- en onderwijsklimaat;

3. Dit protocol bevordert dat de instelling, medewerkers, leerlingen en ouders op de social media communiceren in het verlengde van de missie en visie van de onderwijsinstelling en daarbij de reguliere fatsoensnormen in acht nemen. In de regel betekent dit dat we respect voor de school en elkaar hebben, dat we verdraagzaam zijn en iedereen in zijn waarde laten;
4. De gebruikers van social media dienen rekening te houden met de goede naam van de school en van een ieder die betrokken is bij de school;
5. Het protocol dient ervoor om alle betrokkenen bij de onderwijsinstelling, te beschermen tegen de mogelijke negatieve gevolgen van de social media;

Doelgroep en reikwijdte

1. Deze richtlijnen zijn bedoeld voor alle betrokkenen die deel uitmaken van de schoolgemeenschap, dat wil zeggen medewerkers, leerlingen, ouders/verzorgers en mensen die op een andere manier verbonden zijn aan een van de scholen die resulteren onder de stichting Wijzer aan de Amstel.
2. De richtlijnen in dit protocol hebben alleen betrekking op berichten die gerelateerd zijn aan de stichting, school of wanneer er sprake is een overlap is tussen school, werk en privé.

Social media, de Algemene Verordening Gegevensbescherming (AVG) en de school

A. Voor alle gebruikers (medewerkers, leerlingen en ouders/verzorgers)

1. Het is medewerkers en leerlingen niet toegestaan om tijdens het werk en de lessen actief te zijn op social media, tenzij door de schoolleiding respectievelijk leraren hiervoor vooraf toestemming is gegeven.
2. Het is betrokkenen toegestaan om kennis en informatie over school en de leden van de schoolgemeenschap te delen, mits het geen persoonsgegevens[1] betreft en andere betrokkenen niet schaadt.
3. De betrokkene is persoonlijk verantwoordelijk voor de inhoud die hij[2] publiceert op de social media.
4. Elke betrokkene dient zich ervan bewust te zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na verwijdering van het bericht.
5. De onderwijsinstelling vraagt aantoonbaar schriftelijke toestemming aan medewerkers, en ouders/verzorgers om foto-, film- en geluidsopnamen van aan school gerelateerde situaties, waarop zij zijn afgebeeld, op de school- en/of persoonlijke social media te zetten.
6. Het is medewerkers niet toegestaan om met een privéaccount 'vrienden' te worden van leerlingen en ouders op social media.
7. Alle betrokkenen nemen de reguliere fatsoensnormen tegenover betrokkenen in de onderwijsinstelling in acht. Als fatsoensnormen worden overschreden (bijvoorbeeld: hacken van een account, pesten, kwetsen, stalken, bedreigen, radicalisering, zwartmaken of anderszins beschadigen) dan neemt de onderwijsinstelling passende maatregelen[3].

B. Voor medewerkers tijdens werksituaties

1. Een medewerker kan een professionele groepsapp maken ten behoeve van leerlingen van de klas waaraan hij lesgeeft. Dit ten behoeve van het door hem doorgeven van bijzondere aangelegenheden zoals bij voorbeeld lesuitval, het opgeven van huiswerk, het herinneren aan de gymspullen, schoolreisje, schoolkamp. Die leerlingen die om welke reden dan ook geen deel uit kunnen maken van de groepsapp, worden door de medewerker via de mail op de hoogte gesteld.
2. Medewerkers hebben een bijzondere verantwoordelijkheid bij het gebruik van social media:

[1] „Persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4 AVG).
[2] Voor de leesbaarheid is in de tekst de 'hij' vorm gebruikt. Waarin 'hij' of 'zijn'' staat, kan ook 'zij' of 'haar' worden gelezen. [3] Zie ook: sancties en gevolgen voor medewerkers en leerlingen.

privémeningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de onderwijsinstelling.

Indien een medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met de school waar hij of zij werkzaam is, of gerelateerd kan worden aan een of beide stichtingen dient de medewerker te vermelden dat hij medewerker is van de school en/of de betreffende stichting en welke functie hij heeft.

3. Als online communicatie dreigt te ontsporen dient de medewerker direct contact op te nemen met zijn leidinggevende om de te volgen strategie te bespreken.
4. Bij twijfel of een publicatie in strijd is met deze richtlijnen neemt de medewerker contact op met zijn leidinggevende.

C. Voor medewerkers tijdens privésituaties

1. Het is de medewerker toegestaan om school/werk gerelateerde onderwerpen te publiceren mits het geen persoonsgegevens over haar medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen betreft. Ook mag de publicatie de naam van de school niet schaden.
2. Het is voor medewerkers niet toegestaan standpunten en/of overtuigingen uit te dragen die in strijd zijn met de missie en visie van de school en/of de stichting(en). Daarnaast mogen ze niet in strijd zijn met de uitgangspunten van dit protocol.
3. Indien de medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met de onderwijsinstelling dient hij te vermelden dat hij medewerker is van de school.
4. Als de medewerker over de school en/of stichting(en) publiceert dient hij het bericht te voorzien de mededeling dat de standpunten en meningen in dit bericht de eigen persoonlijke mening zijn (op persoonlijke titel zijn geschreven) en los staan van eventuele officiële standpunten van de school en/of stichting(en).

Sancties en gevolgen voor medewerkers en leerlingen

1. Medewerkers die in strijd handelen met dit protocol maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie over dit onderwerp wordt opgenomen in het personeelsdossier.
2. Indien de directeur-bestuurder en/of de directeur van de school, de wijze van communiceren door een medewerker(s) als ‘grensoverschrijdend’ kwalificeert, dan wordt dit telefonisch gemeld bij de Landelijke Vertrouwensinspecteur (0900 – 1113111).
3. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar medewerkers toe rechtspositionele maatregelen genomen die variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet;
4. Leerlingen en / of ouders/verzorgers die in strijd met dit protocol handelen maken zich mogelijk schuldig aan verwijtbaar gedrag. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het leerlingendossier.
5. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar leerlingen en / of ouders/verzorgers toe maatregelen genomen die onder meer kunnen bestaan uit een waarschuwing, schorsing en verwijdering van school.
6. Wanneer de uitlating van leerlingen en/of ouders/verzorgers en medewerkers mogelijk een strafrechtelijke overtreding inhoudt kan door [naam onderwijsinstelling] aangifte bij de politie worden gedaan.

Dit protocol is met instemming van de (G)MR op 1 januari 2019.

Uithoorn 2019