InformatieBeveiligings- en Privacybeleid (IBP)

Kerobei

Geleding	Meningvormend	Besluitvormend
Directeurenoverleg		
GMR		
Raad van Toezicht		

Inhoudsopgave

1. Het belang van informatiebeveiliging en privacy

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ICT. Deze afhankelijkheid van ICT en gegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy (IBP) om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.
Het schoolbestuur is verantwoordelijk om informatiebeveiliging en privacy te regelen. Het regelen van IBP begint dan ook met een goedgekeurd en bij iedereen bekend gemaakt IBP-beleid. Dat is de basis om processen, richtlijnen en procedures rondom IBP uit te werken.

1.1 Algemene Verordening Gegevensbescherming (AVG).

Het Europees parlement stemde in 2016 in met de **Algemene Verordening Gegevensbescherming** (AVG). Deze nieuwe wetgeving sluit aan op technologische ontwikkelingen en globalisering. Door de AVG zijn persoonsgegevens van alle EU-inwoners straks op dezelfde wijze beschermd, ongeacht of hun gegevens zijn opgeslagen in Europa of - bijvoorbeeld - de Verenigde Staten.
Dat betekent dat er sinds 25 mei 2018 nog maar één privacywet geldt in de hele Europese Unie (EU) als opvolger van de Wet Bescherming persoonsgegevens (WBP).
In de Algemene Verordening Gegevensbescherming (AVG) hebben organisaties die persoonsgegevens verwerken meer verplichtingen. Er wordt in de AVG meer nadruk gelegd op de verantwoordelijkheid van organisaties (scholen) zelf. Scholen moeten niet alleen de **wet naleven**, zij moeten kunnen **aantonen** dat zij zich aan de wet houden.

2. Toelichting informatiebeveiliging en privacy

2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.
Deze aspecten zijn:
Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

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

2.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

2.3 Vervlechting informatiebeveiliging en privacy

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

3. Doelen en reikwijdte

3.1 Doelen

Informatiebeveiliging en privacy heeft de volgende doelen:
Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
Het garanderen van de privacy van alle betrokkenen waarvan Kerobei persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers.
Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers en leerlingen, wordt gerespecteerd en Kerobei voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

Het IBP-beleid binnen Kerobei geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Kerobei waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Kerobei persoonsgegevens verwerkt.

Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Kerobei Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)
Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Kerobei evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

IBP-beleid heeft binnen Kerobei raakvlakken met:

- *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
- *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
- *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
- *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

4. Uitvoering beleid Kerobei - hoe doen we dat?

Het schoolbestuur van Kerobei (in dit hoofdstuk afgekort tot Kerobei) hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

Kerobei neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de ver-werkingsverantwoordelijke.
Informatiebeveiliging Kerobei voldoet aan alle relevante wet- en regelgeving.
Bij Kerobei is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Kerobei om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen te allen tijde hun toestemming herzien.
Kerobei zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
Kerobei legt alle verwerkingen van persoonsgegevens vast in een dataregister of register van verwerkingsactiviteiten en zal deze up-to-date houden. Kerobei voldoet hiermee aan de documentatieplicht.
Binnen Kerobei is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerd systemen

en de daarin opgeslagen informatie, maar ook van papieren documenten.
Kerobei is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
Kerobei classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen, zie hfst 5.5.
Kerobei sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt. Hierbij wordt, indien mogelijk, gebruik gemaakt van de meest recente versie van het convenant Digitale onderwijsmiddelen en privacy (zie bijlage 14.21) en de bijbehorende model verwerkersovereenkomst, zie bijlage 14.20.
Kerobei verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies.
Kerobei heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd, zie bijlage 14.10
Informatiebeveiliging en privacy is bij Kerobei een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
Kerobei kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.
Kerobei neemt i.s.m. de netwerkleverancier passende technische (beveiligings)- maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.
Kerobei zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen In hfst 10.6 staat beschreven hoe een datalek bepaald kan worden en in hfst 10.6 hoe een datalek gemeld moet worden. Zie ook de beslisboom, bijlage 14.18.

5. Uitwerking van het beleid - Wat doen we?

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

5.1 Relevante wet- en regelgeving

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

Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra.
Wet goed onderwijs en goed bestuur PO/VO .
Wet onderwijstoezicht.
Algemene Verordening Gegevensbescherming (AVG).
Archiefwet.
Leerplichtwet.
Auteurswet.
Wetboek van Strafrecht.

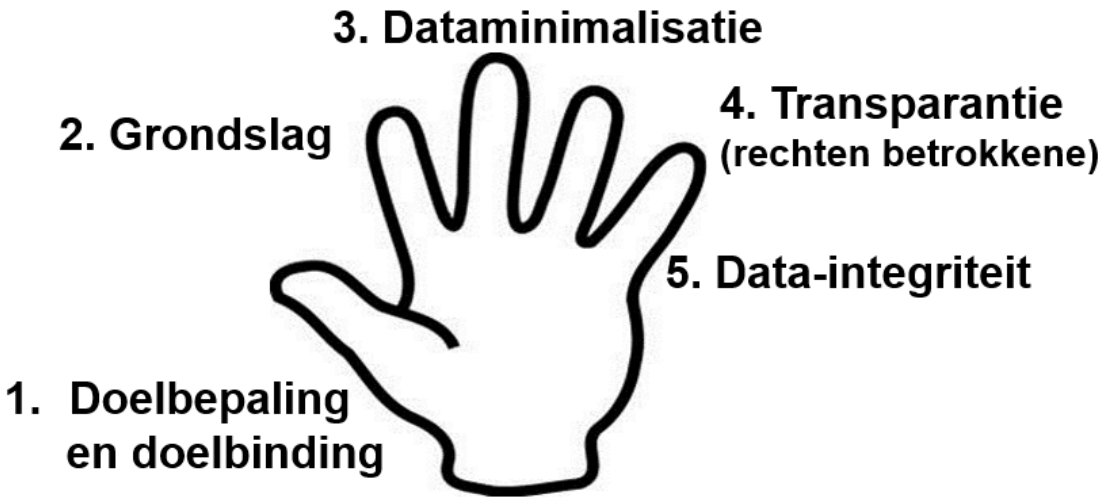
De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' (zie bijlage **14.21**) zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

5.2 Basisregels bij het omgaan met privacy

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een 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. Zie bijlage **14.19**.
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.



5.3 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Deze zijn vermeld als bijlage in dit document. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister of register van verwerkingsactiviteiten.

Kerobei is bezig met het maken van beleid. Dit zal uiterlijk 1-1-2022 toegevoegd worden.

5.4 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de manager IBP (bovenschoolse ICT) met het bestuur als eindverantwoordelijke, zie hfst **6.4.2**.

5.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses, zie bijlage **14.17**.

De gehanteerde classificaties zijn:

- Beschikbaarheid
- Integriteit

- Vertrouwelijkheid

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

Omschrijving classificatie:

Niveau 1	Openbaar, voor iedereen toegankelijk.
Niveau 2	Afgeschermd, voor intern gebruik.
Niveau 3	Vertrouwelijk, voor bepaalde personen.
Niveau 4	Geheim, voor geautoriseerde personen.

Samenvatting risicoanalyse: (meer informatie in bijlage **14.17**.)

Apparatuur	Er is aandacht voor informatiebeveiliging en privacy bij aanschaf en verwijdering van systemen en apparatuur. Leveranciersmanagement (contracten, standaard eisen, controle,).
Diensten	Er is een SLA. Controle en logging.
Gegevens	Er is een risicoanalyse. Medewerkers weten wat persoonsgegevens zijn. Er is een goede back-up/restore voorziening.
Mensen	Medewerkers ondertekenen een gedragscode, zijn op de hoogte van de inhoud en gedragen zich ernaar. Er wordt actief gewerkt aan bewustwording. Er is beleid voor thuiswerken/mobiele devices. Medewerkers weten waar incidenten gemeld moeten worden. Toegangsrechten van gebruikers worden juist ingesteld en geüpdatet. Bij de beëindiging dienstverband worden accounts meteen verwijderd.
Omgeving	Bescherming tegen bedreigingen van buitenaf (brand, overstroming, etc.).
Organisatie	Er is een IBP-plan. Het beleid wordt actief gecommuniceerd. Het beleid wordt minimaal jaarlijks geëvalueerd en wanneer nodig aangepast. Informatieclassificatie (het is duidelijk welke gegevens écht beschermd moeten worden) Er is een toestemmingsbeleid. Taken en verantwoordelijkheden voor IBP zijn duidelijk.
Programmatuur	Met alle leveranciers die persoonsgegevens verwerken wordt een verwerkersovereenkomst afgesloten.

5.6 Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Periodiek worden de beveiligingsincidenten besproken en waar nodig aanvullende passende beleidsmaatregelen genomen. Jaarlijks wordt het incidentenregister geëvalueerd.

Meer informatie in hfst **10**.
In hfst **10.6** staat beschreven hoe een datalek bepaald en gemeld kan worden. Zie ook de beslisboom, bijlage **14.18**.

5.7 Planning en Controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:
De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
de actuele geïnventariseerde risico's;
de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent Kerobei een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

Onderdeel van de planning en control cyclus is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

Voor alle overlegmomenten geldt dat deze zoveel mogelijk ingepast worden in bestaande overlegvormen met hetzelfde karakter waarbij op:

- **Richtinggevend** (strategisch) niveau richtinggevend wordt gesproken over organisatie en compliance, alsmede over doelen, scope en ambitie op het gebied van IBP.
- **Sturend (**tactisch) niveau de strategie wordt vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **Uitvoerend (**operationeel niveau) de onderwerpen worden besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd, en indien nodig in elk organisatieonderdeel van Kerobei.

5.8 Naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP-proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen.

Bij Kerobei wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes enz.
Voor de bevordering van de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol, zie hfst **6.1.1**. De FG is aangesteld door de College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.
Mocht de naleving ernstig tekortschieten, dan kan Kerobei de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.9 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

6. Organisatie - Wie doet wat?

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol.
Dit hoofdstuk beschrijft hoe IBP bij Kerobei 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.

6.1 Rollen (functies) rondom IBP

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Kerobei een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

6.1.1 Functionaris voor Gegevensbescherming

De functionaris (die extern wordt ingehuurd) voor gegevensbescherming (FG) houdt binnen Kerobei toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. De FG heeft regelmatig overleg met de manager IBP. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen. Kerobei heeft een functionaris gegevensbescherming aangesteld vanuit de organisatie Privacy op School (https://www.privacyopschool.nl). Zie bijlage **14.22**.
Zie ook artikel 37 t/m 39 van de AVG.

Korte omschrijving taken Functionaris Gegevensbescherming
Zie WWW: Privacy regulation.eu

1. De functionaris voor gegevensbescherming vervult ten minste de volgende taken:
    a. de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van deze verordening en andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen (Artikel: 35)
    b. toezien op naleving van deze verordening, van andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits; (Artikel: 5)
    c. desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering daarvan in overeenstemming met artikel 35;
    d. met de toezichthoudende autoriteit samenwerken;
    e. optreden als contactpunt voor de toezichthoudende autoriteit inzake met verwerking verband houdende aangelegenheden, met inbegrip van de in artikel 36 bedoelde voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid.

2. De functionaris voor gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

6.1.2 Manager IBP

Adviseert het College van Bestuur en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen Kerobei.

NB. Manager IBP = Bovenschoolse ICT'er (BIC), voorheen stafmedewerker ICT.

6.1.3 Domeinverantwoordelijke (directeur van de school) / proceseigenaar

Binnen de school zijn er verschillende domeinen/processen, zoals ICT, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is de directeur verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

De proceseigenaar is verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:
Samen met het College van Bestuur stellen zij het beleid voor toegang vast.
Samen met functioneel beheer en ICT-beheer zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
Samen met functioneel beheer en ICT-beheer beoordelen zij regelmatig de toegangsrechten van gebruikers.
Leidinggevenden hebben hierin een voorbeeldrol ten opzichte van hun medewerkers.

6.2 Richtinggevend (strategisch)

Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd en bijgesteld. De manager IBP neemt hiertoe het initiatief.

6.3 Sturend (tactisch)

De manager IBP is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op uitvoerend niveau. De manager IBP moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling.
- Draagt zorg voor bijstelling van het IBP-plan (tenminste jaarlijks).
- De uniformiteit bewaken binnen Kerobei
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy.
- De verdere afhandeling van incidenten binnen Kerobei coördineren

6.4 Uitvoerend (operationeel)

6.4.1 Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelshandboek.
Alle medewerkers hebben toegang tot de applicatie “RAP” waarin alle arbeidsvoorwaarden beschreven staan.
Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR)

6.4.2 Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:
er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de manager IBP of door de ICT ambassadeur(s) per school die mede uitvoerend is (zijn) t.a.v. bewustmaking AVG.
Zie bijlage **14.1** voor een schematische weergave.

7. Privacyreglement Kerobei

De huidige versie van het privacyreglement is opgenomen in bijlage **14.2**.
Kerobei heeft ook een privacyverklaring, deze staat op de website.

8. Reglement Internet en sociale media op school

Sociale media spelen een belangrijke rol in het leven van leerlingen, ouders en onderwijzend personeel. Het gebruik van sociale media is onderdeel van het gedrag van leerlingen binnen de school. Sociale media kunnen helpen om het onderwijs te verbeteren en de lessen leuker te maken, om contact te houden met vrienden en te experimenteren en grenzen te verleggen. Maar sociale media brengen ook risico's met zich mee, zoals pesten en het ongewild delen van foto's of andere gegevens. Met dit reglement kan het gesprek op school, in de klas maar ook thuis gevoerd worden over wat er gewoon is op sociale media (en wat niet). De afspraken zijn van toepassing op alle leerlingen van Kerobei, voor het gebruik van mobiele telefoons en sociale media op school en in de klas, maar ook in het mediagebruik buiten de school.

Onder het gebruik van sociale media gaat het om programma's waarmee online informatie kan worden opgezocht, gedeeld en gepresenteerd. Denk bijvoorbeeld aan Facebook, Twitter, Instagram, YouTube, Snapchat maar ook alle (nieuwe) hiermee vergelijkbare programma's en apps.
Voor kinderen onder 16 jaar is toestemming van de ouders nodig voor het gebruik van sociale media.
In bijlage **14.3.1** is een model reglement voor medewerkers en leerlingen **14.3.2** opgenomen dat door de scholen van Kerobei gebruikt wordt.

9. Gedragscode ICT-gebruik en privacy voor personeel Kerobei

9.1 Inleiding

Door het gebruik van ICT wordt het delen van informatie steeds eenvoudiger. Dit biedt allerlei nieuwe mogelijkheden voor bijvoorbeeld het aanbieden van leerstof, het bijhouden van administratie of leerlingendossiers, de registratie van toets gegevens, alsmede de communicatie met leerlingen en ouders.
Hierbij is het van belang dat medewerkers binnen een schoolorganisatie informatie op een goede manier verwerken, zodat:

1. De privacy van leerlingen en personeel wordt gegarandeerd
2. Het imago van de medewerker, de school en Kerobei niet geschaad wordt.

Kerobei wil het gebruik van ICT, waaronder de inzet van sociale media zoveel mogelijk stimuleren en tegelijkertijd medewerkers bewust maken van de mogelijke risico's. Daarbij wordt richting medewerkers duidelijk gemaakt wat van hen verwacht wordt ten aanzien van:

1. De omgang met vertrouwelijke gegevens van leerlingen of medewerkers, waaronder persoonsgegevens, foto's en videomateriaal.
2. De communicatie met derden via sociale media, website, nieuwsbrief, etc.

Deze gedragscode heeft niet alleen betrekking op de digitale verwerking en toegang tot informatie, maar ook betrekking op de 'fysieke omgeving' waarin we gegevens gebruiken en bewaren, zie bijlage **14.10.**
Medewerkers van Kerobei worden geacht ambassadeurs te zijn. De gedragscode dient daarom door iedere medewerker ondertekend te worden. Hiermee laat een medewerker zien professioneel te willen handelen, op de hoogte te zijn van de risico's die betrekking hebben op het verwerken van informatie en het gedrag te vertonen dat nodig is om deze risico's te verminderen.
De gedragscode is geen formaliteit, maar een middel om medewerkers bewust te maken en een aanleiding om met elkaar het gesprek te blijven voeren over de omgang met vertrouwelijke informatie en het gedrag op sociale media. Deze code wordt daarom ook periodiek geagendeerd tijdens ontwikkelingsgesprekken en teamoverleggen.
Naast deze gedragscode neemt Kerobei ook technische maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie zo goed mogelijk te borgen. Dit is uitgewerkt in het informatiebeveiligingsbeleid, zie bijlage **14.11.**
In bijlage **14.14** staat vermeld welke informatie binnen Kerobei wordt verwerkt en gearchiveerd inclusief de wijze waarop dit plaats dient te vinden.

9.2 Omgang met vertrouwelijke gegevens

Binnen Kerobei worden vertrouwelijke gegevens van zowel leerlingen, ouders als personeel verwerkt. Bij leerlingen dient hierbij niet alleen gedacht te worden aan adres- en contactgegevens, toets gegevens, absentie, notities, maar ook medische en andere 'gevoelige' informatie indien dit relevant is voor de onderwijsbegeleiding. Van het personeel worden adres- en contactgegevens bijgehouden, alsmede salarisgegevens en verzuim. Daarnaast wordt in de administratie en communicatie van de scholen foto- en videomateriaal gebruikt van zowel personeel als leerlingen.
Alle vertrouwelijke gegevens worden binnen Kerobei verzameld voor een duidelijk doel. In de schoolgids worden ouders en overige betrokken geïnformeerd welke gegevens door Kerobei verwerkt worden. Voor de verwerking van gegevens zonder een van de wettelijke grondslagen wordt altijd toestemming aan de betrokkene(n) gevraagd. Kerobei heeft de noodzakelijke maatregelen genomen om de gegevens veilig op te slaan en af te schermen voor derden, zoals beveiligde ICT-systemen en fysieke bewaarplaatsen.

9.3 Gedragscode voor medewerkers

Aan alle medewerkers, vaste vervangers, stagiaires, vrijwilligers, ouders in (G)MR en andere personen, ter beoordeling van de directeur, die persoonsgebonden informatie verwerken wordt gevraagd de gedragscode van Kerobei te ondertekenen. Nieuwe medewerkers ontvangen de gedragscode via afdeling Personeelszaken op het stafbureau, de andere hier bovengenoemde personen via de school. Zie bijlage **14.10** De gedragscode is goedgekeurd door de GMR op 25-04-2018.

10. Datalekken en melding hiervan

10.1 Inleiding

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. De meldplicht

geldt voor de verantwoordelijke voor de persoonsgegevens, dat is het schoolbestuur. In overleg moet een verwerker (bijv een leverancier) melding doen aan het bestuur indien het datalek zich heeft voorgedaan bij de verwerker. Dit staat beschreven in de verwerkersovereenkomst.
Het nalaten van deze melding (verantwoordelijke: het bestuur) kan leiden tot een fikse boete.

Kerobei vindt het van groot belang, niet alleen om aan de AVG te voldoen, om de privacy van kind-, ouder- en personeelsgegevens te waarborgen. Belangrijk hierbij is de informatieplicht naar betrokkenen en volledige transparantie over wat scholen vanuit hun professie met gegevens doen en met wie zij deze gegevens delen.

Belangrijke richtsnoeren hierbij zijn:

Rekening houden met wettelijke bewaartermijnen, zie bijlage **14.19**.
Gegevens moeten toereikend zijn, niet overmatig worden verzameld
De gegevens moeten juist en nauwkeurig zijn
Met de gegevens moet vertrouwelijk worden omgegaan
De gegevens moeten goed beveiligd zijn

In dit hoofdstuk beschrijft Kerobei volgens de richtlijnen van de “Autoriteit persoonsgegevens” hoe we als organisatie preventief en curatief om wensen te gaan met het voorkomen en beheersen van “datalekken”.
Van groot belang, is het kweken van bewustzijn onder alle betrokkenen voor “datalekken en bescherming van iemands privacygevoelige gegevens”. Dit is niet alleen een taak van bijvoorbeeld de ICT-afdeling, of loonadministratie of schooldirecteur, maar is een zaak die goed op het netvlies van alle personeelsleden van Kerobei moet komen! Regels en procedures zijn relatief gemakkelijk vast te stellen, maar de mens is in alle beveiligingsissues hier betrekking op hebben de zwakste schakel!

10.2 Preventie

Ondanks alle aandacht voor de beveiliging van systemen kan het voorkomen dat er toch een zwakke plek, een kwetsbaarheid, is. Als iemand een zwakke plek in één van de systemen heeft gevonden is het zaak dat deze binnen 48 uur wordt gemeld (zie bijlage **14.18**) zodat de juiste maatregelen kunnen worden getroffen.
Scholen kunnen dit doen door de bewustwording bij medewerkers en leerlingen te vergroten en het staat hun vrij om hiervoor onderstaande formulieren te gebruiken.
Het “responsible disclosure beleid” heeft als doel om de drempel tot het melden van deze kwetsbaarheden te verlagen, waardoor het beveiligingsniveau van informatiesystemen en het netwerk verhoogd kan worden en schade voor de school kan worden beperkt en/of voorkomen. Voor zowel de school als voor de melder schept het beleid duidelijkheid in de verantwoordelijkheden die beide partijen hebben. Het aanbieden van een beloning kan leerlingen mogelijk (extra) motiveren om een kwetsbaarheid te melden.
Model responsible disclosure voor medewerkers, zie bijlage **14.12**
Model responsible disclosure voor leerlingen, zie bijlage **14.13**

10.3 Wat is een datalek?

Een datalek is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Het is voor de kwalificatie als “inbreuk in verband met persoonsgegevens” niet relevant dat er boos opzet in het spel is. Hoewel een hack van uw systemen waarin persoonsgegevens worden buitgemaakt een schoolvoorbeeld is van een datalek, kunnen ook gegevens die op een verloren laptop staan of een afgesloten website met persoonsgegevens die per ongeluk open staat ook kwalificeren als een datalek.
Zie bijlage **14.18** (beslisboom datalek).

10.4 Meldplicht

Als er sprake is van inbreuken op de beveiliging van persoonsgegevens (een datalek dus), of een vermoeden hiervan, dan moeten deze (vermoedelijke) inbreuken niet alleen worden doorgegeven in het geval van kwaadwillende hackers, maar in alle gevallen waarbij een kans bestaat op nadelige gevolgen voor de privacy van personen.
De inbreuk moet daarvoor wel ‘ernstig’ van aard zijn. Ernstig betekent in dit verband dat er kans is op verlies of onrechtmatige verwerking van persoonsgegevens. Dit blijft een case-by-case inschatting die de school en het CvB Kerobei zelf zal moeten maken, maar bijvoorbeeld het “kwijtraken” van een zorgdossier van een kind of een personeelsdossier moet worden gezien als ernstig!
De meldplicht is bovendien tweeledig. Er moet in ernstige gevallen gemeld worden aan de Autoriteit persoonsgegevens en in sommige gevallen aan alle betrokkenen. De melding van een datalek moet zo spoedig mogelijk na het voorval worden gedaan (binnen 48 uur intern Kerobei en 72 uur bij de Autoriteit Persoonsgegevens), tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de betrokkene(n). Als het datalek waarschijnlijk een hoog risico inhoudt voor de betrokken(n) dan dient men naast de Autoriteit Persoonsgegevens ook de betrokkenen in te lichten. Indien een datalek onterecht niet aan de AP en/of betrokkene(n) gemeld wordt, dan riskeert Kerobei een boete tussen de 300.000 en 750.000 Euro.
Zie Staatscourant maart 2019 *Boetebeleidsregels AP*.

10.5 In de praktijk

Bovenstaande betekent in de praktijk dat moet worden opgelet in ten minste deze gevallen:
Verlies of diefstal van o.a. een USB-stick, een computer, laptop, tablet, telefoon, documenten (aktentas, schooltas) of van wachtwoorden waarmee privacygevoelige informatie is te achterhalen.
Privacygevoelige informatie is o.a.: Burger Service Nummers (BSN), kopieën van identiteitsbewijzen, informatie over iemands godsdienst, levensovertuiging, seksuele geaardheid, strafrechtelijke gegevens, salarisgegevens, schulden, politieke overtuiging, prestaties op school of werk- of relatieproblemen.

Situaties waarbij er niet veilig wordt omgegaan met persoonsgegevens, die kunnen leiden tot een datalek (zie ook de beslisboom datalekken, bijlage **14.18** en de gedragscode, bijlage **14.10**):

Niet afgesloten dossierkasten die voor onbevoegden toegankelijk zijn
Formulieren of documenten die op bureaus rondslingeren (clean desk policy dient overal te gelden!)

Niet opgehaalde afdrukken op de printer/kopieerapparaat
‘Openstaande’ beeldschermen van de computer bij afwezigheid (op school/kantoor, maar ook extern via telewerk-omgeving)
Werken in een open(bare) Wifi-verbinding
Wachtwoorden die op het bureau of thuis makkelijk te vinden zijn (op papier/in agenda)
Wachtwoorden die door derden worden afgekeken
Inloggegevens die worden uitgeleend
Foutief geadresseerde e-mails
Mailen van kind gegevens

10.6 Bepaling datalek en meldprocedure

Als er sprake is van een datalek (of men vermoedt een datalek) zoals in voornoemde tekst besproken, neem dan eerst contact op met de directeur van de school. Deze neemt vervolgens **binnen 48** uur contact op, telefonisch of per mail, met de manager IBP.
Tot 1-8-2021: Ton Pouls, 077-396 8888, 0613651927, privacymelding@kerobei.nl
Vanaf 1-8-2021: René van Ewijk 077-396 8888, 06 5474 8550, privacymelding@kerobei.nl
In overleg zal bekeken worden hoe de procedure vervolgd wordt. Maak bij vermoedelijke datalekken of incidenten gebruik van het meldingsformulier Zie Beslisboom meldingsformulier Incidenten en datalekken versie 1 (BK - AVG-Kerobei en privacy).
Bij vermeende datalekken op het stafbureau dient meteen contact te worden opgenomen met het CvB.

(zie de beslisboom datalekken, bijlage **14.18**

11. Informeren van ouders

Bij Kerobei wordt zorgvuldig omgegaan met de privacy van onze leerlingen. In verband met het geven van onderwijs, het begeleiden van onze leerlingen, en de vastlegging daarvan in de administratie van onze scholen, 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 scholen van Kerobei maken ook gebruik van digitaal leermateriaal. De leveranciers van die leermaterialen ontvangen een beperkt aantal leerling gegevens. Kerobei heeft met haar leveranciers strikte afspraken gemaakt over het gebruik van persoonsgegevens, zodat misbruik wordt voorkomen. Leerling informatie wordt alleen gedeeld met andere organisaties als ouders daar toestemming voor geven, tenzij die uitwisseling verplicht is volgens de wet.

In het privacyreglement bijlage **14.2** is beschreven hoe de scholen van Kerobei omgaan met de leerling gegevens, en wat de rechten zijn van ouders en leerlingen. Natuurlijk kunnen ouders voor vragen ook terecht bij de directie van de betreffende school.

11.1 Wettelijke informatieplicht aan ouders

In de wet is bepaald dat organisaties zoals Kerobei informatieplicht hebben. Ouders worden uiteraard geïnformeerd indien zij betrokken raken bij een datalek.
Zie schema in bijlage **14.15**.

11.2 Welke gegevens bewaren scholen van Kerobei

De basisscholen bewaren verschillende gegevens over kinderen in een leerling dossier. De school en ouders mogen deze leerling gegevens inzien. In speciale gevallen mogen derden dat ook.

Zie bijlage **14.14**.
De teksten kunnen door de scholen gebruikt worden voor informatie aan ouders.

11.3 Welke rechten hebben ouders, leerlingen en derden (betrokkenen)

Transparantie is voor Kerobei een belangrijke privacy-waarde. Ouders en leerlingen worden actief betrokken. Kerobei stelt betrokkenen in staat om bezwaren te uiten en hun rechten uit te oefenen. Deze rechten zijn vastgelegd in de wet en zijn beschreven in bijlage **14.16**

11.4 Het verlenen van toestemming door ouders en/of verzorgers

Ouders kunnen toestemming verlenen voor bepaalde zaken d.m.v. een handtekening op een (papieren) formulier of via een ouderapp. Het bewijs dat toestemming is verkregen is vormvrij. Je moet kunnen aantonen dat de toestemming middels een actieve handeling van de betrokkene is verkregen. De betrokkenen moeten wel geïnformeerd zijn (in eenvoudige taal) waar ze precies toestemming voor geven en dat ze hun rechten kunnen nalezen in de privacyverklaring op de website van Kerobei. Zie hfst **14.8.5** voor toestemming door 1 of 2 ouders.

11.5 Recht op intrekking verleende toestemming

Ouders/verzorgers kunnen te allen tijde en zonder opgaaf van redenen de toestemming m.b.t. het gebruik van sociale media en beeldmateriaal intrekken. Dit dient schriftelijk te gebeuren middels het formulier *Intrekking toestemming gebruik beeldmateriaal en sociale media*, voorzien van naam, datum en handtekening, zie hfst **14.8.13** .
Elke school is verplicht ouders te wijzen op het recht tot intrekking van de toestemming. Dit kan via de ouderapp, website, nieuwsbrief en/of schoolgids. Hierdoor hoeft er niet elk jaar om toestemming worden gevraagd.

11.6 Monitoring motorische ontwikkeling (MQ-scan - alleen gemeente Venlo)

Op de scholen in de gemeente Venlo wordt elk jaar de motorische ontwikkeling gemonitord.
Hiervoor heeft Kerobei een overeenkomst afgesloten met de gemeente Venlo:
(Gedeelde drives\BK - AVG - Kerobei en privacy\Verwerkersovereenkomsten\MQscan…)

Hiervoor moet toestemming gevraagd worden aan de ouders. Zie hfst **14.8.12** voor het toestemmingsformulier.
Aangezien deze monitor geanonimiseerd wordt afgenomen vindt er geen inbreuk plaats op privacy gegevens. Deze passage is expliciet opgenomen binnen het privacyreglement van Kerobei.

11.7 Passend onderwijs, jeugdhulpverlening

Hiervoor gelden andere regels en bewaartermijnen. In uitvoering, uiterlijk x-x-2021.

11.8 Digitaal thuisonderwijs (reglement)

Met de komst van digitaal thuisonderwijs, bijv. bij schoolsluiting of het thuis digitaal volgen door leerlingen van de lessen op school zijn er veel nieuwe situaties en uitdagingen met betrekking tot privacy ontstaan. Dit reglement heeft als doel de privacy van leerlingen en leerkrachten te waarborgen.
Dit reglement is van toepassing voor leerlingen, ouders/verzorgers, alle andere aanwezigen in de thuissituatie en betrokken medewerkers van de scholen.

Wettelijke kaders:

- het is verboden om opnames te maken van lessen die online gevolgd worden.
- het is niet toegestaan om beeld of geluid van de lessen of andere digitale contacten tussen school en leerlingen/ouders/verzorgers te verspreiden, te bewerken en/of te delen op internet en/of social media.
- het is verboden om schermafbeeldingen van video- en/of chatgesprekken met leerkrachten en andere leerlingen te maken.
- in principe volgen alleen de leerlingen zelf de lessen; toehoorders zijn, net als in een gewone les, in beginsel niet gewenst. Alleen in overleg met de school kan hiervan worden afgeweken.
- de reguliere gedragsregels die gelden voor fysiek onderwijs zijn ook van toepassing op digitaal thuisonderwijs.

Voorbeeld tekst voor te hanteren regels op scholen:

Regels digitaal onderwijs:

- check regelmatig je mail in verband met uitnodigingen of informatie die de juf of meester je toestuurt.
- zorg dat je 2 minuten voor de afgesproken MEET tijd on-line bent.
- zorg voor een ruimte waarin je je zo goed mogelijk kunt concentreren (spreek dit af met je ouders of leerkracht).
- we MEETEN niet met andere kinderen in dezelfde ruimte.
- we MEETEN in “gewone kleren” die we ook naar school aandoen.
- we MEETEN aan een tafel of een bureau en zitten op een stoel.
- standaard staat je eigen speaker of geluid UIT.
- je camera staat altijd AAN.
- gebruik de chat (als deze aan staat) altijd respectvol en zorg dat jouw berichten te maken hebben met het onderwerp wat aan bod is.
- ..... (per school de mogelijkheid om zelf aan te vullen)

12. Aanmeldingsformulier en toestemming publicatie foto-video

12.1 (Voor)aanmeldingsformulier

Het (Voor)aanmeldingsformulier is aangepast aan de AVG. Elke school kan eigen, specifieke, informatie toevoegen. Zie bijlage **14.9**.

Toelichting:

Het is erg belangrijk dat o.a. de NAW gegevens van ouders en leerlingen foutloos in het LVS (ParnasSys) opgenomen worden. Het is niet toegestaan om een kopie van het ID te vragen en dat te bewaren in het dossier.
Optionele werkwijze m.b.t. persoonsgegevens van ouders en leerlingen:
Je kunt je een kopie van het ID vragen voor een afgesproken periode van maximaal een week. Alleen degene die de inschrijving regelt, mag dit document inzien. De kopie moet tot de inschrijving is afgerond, veilig opgeborgen worden in een afsluitbare ruimte of kast. Na de inschrijving moet de kopie teruggegeven of vernietigd worden.
Let op: voor medewerkers gelden andere regels: het opslaan van een kopie van het ID-bewijs in het personeelsdossier is verplicht.

12.2 Toestemming publicatie beeldmateriaal (foto's en video's)

Op scholen worden ten behoeve van informatievoorziening en communicatie op de website, in nieuwsbrieven of ouderportalen ook foto's of video's getoond waarop kinderen en personeel van scholen is te zien. Hiervoor dient vooraf en ieder schooljaar opnieuw, toestemming worden verleend door ouders. Het is ook mogelijk om ouders op niet mis te verstane wijze te informeren via bijv. de website, ouderportaal/app, schoolgids... dat ze hun goedkeuring te allen tijde kunnen intrekken. Vanzelfsprekend is toestemming in vrijheid gegeven en geldt ondubbelzinnig voor een vooraf gesteld doel. Zie hfst **14.8.13**

Een format met een voorbeeldtekst dat scholen kunnen gebruiken om ouders hieromtrent te informeren is te vinden in bijlage **14.4**.
Een toestemmingsformulier dat gebruikt kan worden om ouders te laten ondertekenen, of toestemming in te trekken is te vinden in bijlage **14.8.13**
Toelichting toestemmingsformulier, zie bijlage **14.6**

Voorbeeldtekst voor schoolgids en ouderportaal/app:
Zie hfst **14.8.13**

13. Toegangsbeleid Kerobei

Inleiding

Door de digitalisering is de hoeveelheid informatie en opslag- of bewaarplaatsen binnen een onderwijsorganisatie enorm toegenomen. Informatie kan ook eenvoudiger gedeeld worden, waardoor

meerdere bronnen gebruikt worden voor dezelfde informatie. De school is verantwoordelijk voor een aantal wettelijke taken zoals de bescherming van privacygevoelige gegevens. Daarom is het belangrijk dat schoolbesturen aan de slag gaan met toegangsbeleid. Dit betreft het bepalen, het verlenen en controleren van toegangsrechten.
Om toegangsrechten te kunnen bepalen is het van belang dat er geïnventariseerd wordt welke gegevens door wie mogen worden ingezien, geregistreerd/gewijzigd of verwijderd. Hierbij is het van belang om onderscheid te maken in de privacy gevoeligheid van informatie (zie bijlage 5.5 classificatie en risicoanalyse).

Inventarisatie

Hieronder is per systeem aangegeven welke gegevens dit bevat en wat de toegangsrechten zijn met betrekking tot deze gegevens. Daarnaast is per systeem aangegeven wat de Privacy classificatie is van de gegevens en daaraan gerelateerd:

1. wie de accounts verstrekt/intrekt
2. op welke wijze de accounts worden verstrekt
3. hoe vaak de toegangsrechten worden gecontroleerd
4. welke toegangsmiddel wordt gebruikt
5. sterkte van het wachtwoord
6. hoe vaak het wachtwoord moet worden ververst

Er wordt onderscheid gemaakt in de volgende rollen:

- CvB (cvb)
- manager IBP (MIBP)
- Directie (D)
- Teamleider (TL)
- ICT-beheerder school (BS)
- Administratief personeel (AP)
- Onderwijs personeel (OP)
- Onderwijs personeel tijdelijk (OPT), denk aan invalkrachten, stagiaires, etc.
- Leerlingen (L)
- Ouders/verzorgers (O)
- Netwerkleverancier (NL)
- Verwerker (V)
- Externen (E)

13.1 Wachtwoordbeleid

Afspraken:
Een wachtwoord moet voldoen aan volgende eisen: tenminste 10 karakters, 1 hoofdletter, 1 kleine letter en 1 cijfer. Dit geldt als een programma dat toelaat. Sommige programma's laten bijv. geen of niet alle symbolen toe. De combinatie van de karakters mag niet gemakkelijk te raden zijn (1Janssen!). Sommige programma's en diensten hebben eigen voorwaarden en accepteren ook wachtwoorden die aan mindere dan bovenstaande specificaties voldoen. De afspraken over wachtwoorden binnen Kerobei gelden ook hier, al kan dit niet door Kerobei gecontroleerd worden.

Aanbevolen:

Gebruik een zin: Ckjwi5sawhtki! = Computers kunnen je wachtwoord in 5 seconden achterhalen wanneer het te kort is!
Een wachtwoord wordt niet gedeeld.
Een wachtwoord wordt minimaal een keer per jaar veranderd.
Een wachtwoord wordt niet hergebruikt.
Gebruik voor elk programma een eigen wachtwoord.
Gebruik voor leerlingen in de onderbouw, indien mogelijk, een combinatie van afbeeldingen.

Ivm de privacy en veiligheid (AVG) is het belangrijk het scherm te vergrendelen als je niet bij de pc aanwezig bent.
Schermvergrendeling op de Chromebooks: zoeken-L; bij Windows is dit Windowstoets-L

13.1.1 Bewaren van wachtwoorden

Kerobei is op zoek naar een wachtwoordkluis. Zolang deze niet beschikbaar is moeten de wachtwoorden in een beveiligd Office-document bewaard worden.

Open een nieuw bestand in WORD of Excel:
Klik op *Bestand, Info, Document/werkmap beveiligen, Versleutelen met wachtwoord.* Type het wachtwoord in*, Ok,* Type wachtwoord opnieuw in*, Ok.*

13.2 Autorisatie matrix

Alle verwerkingen van persoonsgegevens binnen of ten behoeve van de schoolorganisatie moeten worden gedocumenteerd.
Kerobei is bezig met het maken van beleid. Dit zal in 2021 toegevoegd worden.

13.3 Documentatieplicht

Kerobei houdt een register van alle verwerkingsactiviteiten bij. Dit zal in 2021 bijgewerkt worden.

14. Bijlagen

14.1 Rollen, taken en verantwoordelijkheden

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	CvB Kerobei	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen

		verwerken van persoonsgegevens ● Evalueren toepassing en werking IBP-beleid op basis van rapportages ● Organisatie IBP inrichten	● Reglement FG vaststellen ● Privacyreglement vaststellen
Sturend (tactisch)	(Manager IBP)	● Inhoudelijk verantwoordelijk voor IBP ● IBP-planning en controle ● Adviseert bestuur/CvB/directie over IBP ● Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse ● Hanteren IBP normen en wijze van toetsen ● Evalueren IBP-beleid en maatregelen ● Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze ● Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Processen, richtlijnen en procedures IBP, waaronder: ● activiteitenkalender ● Protocol beveiligingsincidenten en datalekken ● Verwerkersovereenkomsten regelen ● Brief toestemming gebruik foto's en video ● Opstellen informatie documentatie richting leerlingen, ouders / verzorgers ● Security awareness activiteiten ● Sociale media reglement ● Gedragscode ict en internetgebruik ● Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming (FG) manager IBP	● Toezicht op naleving privacy wetgeving ● Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens ● Afwikkeling klachten en incidenten	● Privacyreglement, ● procedure IBP-incident afhandeling ● Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proces-eigenaren waaronder: ict, personeel (HRM / P&O), Facilitair,	● **Classificatie / risicoanalyse** *in samenwerking met manager IBP (verantwoordelijke IBP)* ● Toegangsbeleid zowel fysiek als digitaal vaststellen en	● Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) ● Classificatie- en risicoanalyse documenten.

	onderwijs, financiën, inkoop en administratie manager IBP	laten goedkeuren door *bestuur/CvB/directie* ● *Samen met functioneel beheer en ICT beheer* er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. ● *Samen met functioneel beheer en ICT* beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: ● Toegangsmatrix diverse informatiesystemen en netwerk
Uitvoerend (operationeel)	manager IBP Functioneel beheerder: Cloudwise Medewerker directeur	● Incidentafhandeling (registreren en evalueren). ● Technisch aanspreekpunt voor IBP-incidenten. ● Uitvoeren taken conform gegeven richtlijnen en procedures. ● Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. ● 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.	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

		• 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.	

Opmerking. In een aantal gevallen is ook de (G)MR betrokken.

14.2 Privacyreglement Kerobei

1. Toepasselijkheid	Dit reglement geldt voor de gehele organisatie die deel uitmaakt van Kerobei stichting voor primair onderwijs met scholen in Baarlo, Beesel, Belfeld, (Hout)-Blerick, Maasbree, Reuver, Steyl en Tegelen. Wylrehofweg 11, 5912PM Venlo. 077-3968888
2. Definities	
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‘de betrokkene’), zoals bijvoorbeeld naam, adres, geboortedatum, titel(s), geslacht, adres, telefoonnummer, e-mailadres, functie, personeelsnummer, medische rapportages, inhoud van e-mails, prestaties/cijfers, brieven, klachten, foto’s, video’s, IP-adressen, tracking cookies, loginnamen en wachtwoorden.
Verwerking van persoonsgegevens	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, geautomatiseerd of handmatig, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Bijzondere persoonsgegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische gegevens (DNA/RNA) of biometrische gegevens (bijv. foto’s) met het oog op de unieke identificatie van een persoon, en gegevens over gezondheid, of iemands seksueel gedrag of seksuele gerichtheid.

Betrokkene	Degene op wie een persoonsgegeven betrekking heeft, en die al dan niet wordt vertegenwoordigd door een wettelijk vertegenwoordiger. Betrokkenen kunnen bijvoorbeeld zijn: leerlingen, ouders, medewerkers en bezoekers.
Wettelijk vertegenwoordiger	Degene die het ouderlijk gezag over een minderjarige uitoefent. Meestal zal dit een ouder zijn, maar het kan ook gaan om een voogd.
Verwerkingsverantwoordelijke	De entiteit die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit reglement is het Bevoegd gezag, te weten Kerobei, vertegenwoordigd door het College van Bestuur, de verwerkingsverantwoordelijke.
Verwerker	De natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke (Kerobei) persoonsgegevens verwerkt, zoals bijvoorbeeld de leverancier van een leerlingvolgsysteem of leerling-administratiesysteem. Een verwerker heeft een uitvoerende taak, ten behoeve van de activiteiten van de verwerkingsverantwoordelijke.
Derde	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, de verwerkingsverantwoordelijke, de verwerker, of de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken.
BEVOEGD GEZAG	Kerobei, de verwerkingsverantwoordelijke in de zin van dit reglement.
3. Reikwijdte en doelstelling	1. Dit reglement stelt regels over de verwerking van persoonsgegevens van alle betrokkenen bij de organisatie, waaronder leerlingen en hun wettelijk vertegenwoordigers, medewerkers, bezoekers en externe relaties (bijv. leveranciers en opdrachtnemers). 2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door Kerobei worden verwerkt. Het 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 met welk doel en op welke (juridische) grondslag persoonsgegevens binnen Kerobei worden verwerkt; c. ook overigens te borgen dat persoonsgegevens binnen Kerobei rechtmatig, transparant en behoorlijk worden verwerkt; d. de rechten van betrokkenen vast te leggen en te borgen dat deze rechten door Kerobei worden gerespecteerd.
4. Doelen van de verwerking van persoonsgegevens	Bij de verwerking van persoonsgegevens houdt Kerobei zich aan de relevante wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG), de uitvoeringswet AVG en de onderwijswetgeving.
Doelen	1. De verwerking van persoonsgegevens vindt plaats voor:

	a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, het voorzien in hun (extra) ondersteuningsbehoefte, dan wel het geven van studieadviezen; b. het verstrekken en/of ter beschikking stellen van leermiddelen; c. het bewaken van de veiligheid binnen de scholen en het beschermen van eigendommen van medewerkers, leerlingen en bezoekers; d. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld, onder a en b, alsmede van informatie over de leerlingen op de eigen website; e. het bekend maken van de activiteiten van de organisatie, bijvoorbeeld op de website van Kerobei of van de scholen, in brochures of de schoolgids of via social media; f. het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen; g. het aanvragen van bekostiging, het behandelen van geschillen daarover en het doen uitoefenen van accountantscontrole; h. het onderhouden van contacten met oud-leerlingen; i. het aangaan en uitvoeren van arbeidsovereenkomsten, samenwerkingsrelaties met opdrachtnemers en contracten met leveranciers; j. de uitvoering of toepassing van wet- en regelgeving; k. juridische procedures waarbij Kerobei betrokken is. 2. De verwerking van persoonsgegevens mag ook plaatsvinden voor doelen die verenigbaar zijn met de doelen zoals beschreven in lid 1.
5. Doelbinding	Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. Kerobei verwerkt niet meer gegevens dan noodzakelijk is om de betreffende doelen te bereiken.
6. Soorten persoonsgegevens	De categorieën van persoonsgegevens zoals deze binnen Kerobei worden verwerkt, worden geregistreerd in een verwerkingsregister.
7. Grondslag verwerking	Verwerking van persoonsgegevens gebeurt alleen indien aan een van de onderstaande voorwaarden is voldaan: a. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan Kerobei is opgedragen. a. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op Kerobei rust. a. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de arbeidsovereenkomst) of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen. a. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van Kerobei of van een derde, behalve wanneer

	de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen, met name wanneer de betrokkene een kind is; in het kader van deze grondslag zal dus een belangenafweging moeten plaatsvinden. a. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen (levensbelang) a. De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.
9. Bewaartermijnen	Kerobei bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor deze worden verwerkt, tenzij het langer bewaren van de persoonsgegevens op grond van wet- of regelgeving verplicht is.
10. Toegang	Binnen de organisatie van Kerobei geldt dat personen slechts toegang hebben tot persoonsgegevens voor zover dat daadwerkelijk nodig is. De toegang van medewerkers tot persoonsgegevens is dan ook beperkt tot de gegevens die noodzakelijk zijn voor de goede uitoefening van hun functie en (dus) hun werkzaamheden. Verder wordt slechts toegang verschaft tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan: a. de verwerker die van Kerobei de opdracht heeft gekregen om persoonsgegevens te verwerken, maar alleen voor zover dat noodzakelijk is in het licht van de gemaakte afspraken; b. derden voor zover uit de wet voortvloeit dat Kerobei verplicht is om toegang te geven of sprake is van een (andere) grondslag voor deze verwerking, bijvoorbeeld de vervulling van een taak van algemeen belang.
11. Beveiliging en geheimhouding	1. Kerobei neemt passende uitwisselene en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. Deze maatregelen zijn er mede op gericht om niet noodzakelijke verzameling en verdere (niet noodzakelijke) verwerking van persoonsgegevens te voorkomen. 2. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen. 3. Eenieder die betrokken is bij de verwerking van persoonsgegevens binnen Kerobei is verplicht tot geheimhouding van de betreffende persoonsgegevens, en zal deze gegevens slechts verwerken voor zover dat noodzakelijk is voor de uitoefening van de betreffende functie, werkzaamheden of taak.
12. Verstrekken gegevens aan derden	Kerobei kan persoonsgegevens aan derden verstrekken als daarvoor een grondslag bestaat in de zin van artikel 7 van dit reglement.

13. Sociale media	Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het sociale mediaprotocol van Kerobei.
14. Rechten betrokkenen	1. Kerobei erkent de rechten van betrokkenen, handelt daarmee in overeenstemming en bewerkstelligt dat betrokkenen deze rechten daadwerkelijk kunnen uitoefenen. Het betreft in het bijzonder de volgende rechten:
Inzage	a. Een betrokkene heeft recht op inzage van de door Kerobei verwerkte persoonsgegevens die op hem betrekking hebben, behalve voor zover het gaat om werkdocumenten, interne notities en andere documenten die uitsluitend bedoeld zijn voor intern overleg en beraad. Indien en voor zover dit recht op inzage ook de rechten en vrijheden van anderen raakt, bijvoorbeeld als in de documenten ook persoonsgegevens van anderen dan de betrokkene zijn vermeld, kan Kerobei het recht op inzage beperken. Bij het verstrekken van de betreffende gegevens verschaft Kerobei voorts informatie over: ● de verwerkingsdoeleinden; ● de categorieën van persoonsgegevens die worden verwerkt; ● de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt; ● (indien van toepassing) ontvangers in derde landen of internationale organisaties; ● (indien mogelijk) hoe lang de gegevens worden bewaard; ● dat de betrokkene het recht heeft om te verzoeken dat de persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van de persoonsgegevens wordt beperkt, alsmede dat hij het recht heeft om bezwaar te maken tegen de verwerking van de persoonsgegevens; ● het feit dat de betrokkene een klacht kan indienen bij de Autoriteit Persoonsgegevens; ● de bron van de persoonsgegevens, indien de persoonsgegevens niet van de betrokkene zelf zijn verkregen; ● het eventueel toepassen van geautomatiseerde besluitvorming en de betreffende onderliggende logica en het belang en de gevolgen voor de betrokkene; ● de passende waarborgen indien de persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie.
Verbetering, aanvulling, verwijdering	b. Kerobei verbetert de persoonsgegevens van een betrokkene in het geval de betrokkene terecht heeft aangegeven dat de gegevens onjuist zijn, en Kerobei vult de persoonsgegevens van een betrokkene aan indien de betrokkene terecht om aanvulling heeft verzocht. Voorts kan de betrokkene verzoeken om verwijdering van zijn persoonsgegevens. Kerobei gaat daartoe over indien is voldaan aan een wettelijke grondslag voor het verzoek, tenzij het onmogelijk

	is om aan het verzoek te voldoen of dit een onredelijke inspanning zou vergen.
Bezwaar *Beperken verwerking* *Kennisgevingsplicht*	c. Indien Kerobei persoonsgegevens verwerkt op de grondslag van artikel 7 onder a of artikel 7 onder d van dit reglement, kan de betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens. In dat geval staakt Kerobei de verwerking van de betreffende persoonsgegevens, behalve als naar het oordeel van Kerobei het belang van Kerobei, het belang van derden of het algemeen belang in het betreffende concrete geval zwaarder weegt. d. De betrokkene kan voorts verzoeken om de verwerking van zijn persoonsgegevens te beperken, namelijk indien hij een verzoek tot verbetering heeft gedaan, indien hij bezwaar heeft gemaakt tegen de verwerking, als de persoonsgegevens niet meer nodig zijn voor het doel van de verwerking of als de gegevensverwerking onrechtmatig is. Kerobei staakt dan de verwerking, tenzij de betrokkene toestemming heeft gegeven voor de verwerking, Kerobei de gegevens nodig heeft voor een rechtszaak of de verwerking nodig is ter bescherming van de rechten van een andere persoon of vanwege gewichtige redenen. e. Als Kerobei op verzoek van een betrokkene een verbetering of verwijdering van persoonsgegevens heeft uitgevoerd, of de verwerking van persoonsgegevens heeft beperkt, zal Kerobei eventuele ontvangers van de betreffende persoonsgegevens daarover informeren.
Procedure	2. Kerobei handelt een verzoek van een betrokkene zo spoedig mogelijk, maar uiterlijk binnen een maand na ontvangst van het verzoek, af. Afhankelijk van de complexiteit en van het aantal verzoeken kan die termijn indien nodig met twee maanden worden verlengd. Als deze verlenging plaatsvindt, wordt de betrokkene daarover binnen een maand na de ontvangst van het verzoek geïnformeerd. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt. Wanneer Kerobei geen gevolg geeft aan het verzoek van de betrokkene, deelt Kerobei onverwijld en uiterlijk binnen een maand na ontvangst mede waarom het verzoek niet wordt ingewilligd en informeert hij de betrokkene over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of beroep bij de rechter in te stellen.
Intrekken toestemming	3. Indien voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijde door de betrokkene of zijn wettelijk vertegenwoordiger worden ingetrokken. Als de toestemming wordt ingetrokken, staakt Kerobei de verwerking van persoonsgegevens, behalve als er een andere grondslag (zoals bedoeld in

	artikel 7) voor de gegevensverwerking is. Het intrekken van de toestemming tast de rechtmatigheid van verwerkingen die reeds hebben plaatsgevonden niet aan.
15. Transparantie	Kerobei informeert de betrokkene(n) actief over de verwerking van hun persoonsgegevens, in ieder geval door middel van een laagdrempelige privacyverklaring. In de privacyverklaring wordt in ieder geval de volgende informatie vermeld: a) de contactgegevens van Kerobei; b) de contactgegevens van de functionaris voor gegevensbescherming van Kerobei; c) de doeleinden van de gegevensverwerking en de grondslagen voor de verwerking; d) een omschrijving van de belangen van Kerobei indien de verwerking wordt gebaseerd op het gerechtvaardigd belang van Kerobei; e) de (categorieën) ontvangers van de persoonsgegevens, zoals verwerkers of derden; f) in voorkomend geval: of de persoonsgegevens worden verzonden aan landen buiten de Europese Economische Ruimte (EER); g) hoe lang de persoonsgegevens zullen worden bewaard; h) dat de betrokkene het recht heeft om Kerobei te verzoeken om inzage, verbetering of verwijdering van persoonsgegevens, en dat hij het recht heeft om te verzoeken om beperking van de verwerking, om bezwaar te maken of om een beroep te doen op het recht van gegevensoverdraagbaarheid; i) dat de betrokkene het recht heeft om zijn toestemming in te trekken, als de gegevensverwerking is gebaseerd op toestemming; j) dat de betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens; k) of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te kunnen sluiten, en of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de gevolgen zijn indien hij de persoonsgegevens niet verstrekt; l) het bestaan van geautomatiseerde besluitvorming, vergezeld van nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.
16. Meldplicht datalekken	Eenieder die betrokken is bij een verwerking van persoonsgegevens is verplicht om een datalek per ommegaande te melden bij het meldpunt (privacymelding@kerobei.nl), conform het protocol beveiligingsincidenten en datalekken van Kerobei. Een datalek is elke inbreuk waarbij persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk zijn gemaakt.
17. Klachten	1. Wanneer een betrokkene van mening is dat het doen of nalaten van Kerobei niet in overeenstemming is met de AVG, dit reglement of (andere) toepasselijke wet- of regelgeving, dan kan een klacht worden ingediend overeenkomstig de binnen Kerobei geldende klachtenregeling. Een

	betrokkene kan zich eveneens wenden tot de functionaris voor gegevensbescherming van Kerobei. 2. Als een klacht naar de mening van betrokkene door Kerobei niet correct is afgewikkeld, kan hij zich wenden tot de rechter of de Autoriteit Persoonsgegevens.
18. Onvoorziene situatie	Indien zich een situatie voordoet die niet beschreven is in dit reglement, neemt het College van Bestuur van Kerobei de benodigde maatregelen, en wordt beoordeeld of dit reglement dientengevolge moet worden aangevuld of aangepast.
19. Wijzigingen reglement	1. Dit reglement is na instemming van de Gemeenschappelijke Medezeggenschapsraad (GMR) vastgesteld door het College van Bestuur van Kerobei. Het reglement wordt gepubliceerd op de website van Kerobei en de websites van de scholen. Het reglement wordt verder actief onder de aandacht gebracht, bijvoorbeeld door middel van verwijzing in de schoolgids. 2. Het College van Bestuur kan dit reglement wijzigen na instemming van de GMR.
20. Slotbepaling	Dit reglement wordt aangehaald als het privacyreglement van Kerobei en treedt in werking op 25-04-2018**.**

14.3 Modelreglementen Internet en sociale media

(bron: Kennisnet).
Scholen van Kerobei moeten onderstaande modelreglementen gebruiken, aanpassen of uitbreiden.

14.3.1 Bewaren van wachtwoorden

Social Media zijn niet meer weg te denken in onze maatschappij en dus ook niet bij iedereen die betrokken is in het onderwijs. Social media kunnen een goede bijdrage leveren aan de professionaliteit van onderwijspersoneel en de kwaliteit van het onderwijs. Net zoals bij de introductie van internet en e-mail eind vorige eeuw levert het gebruik van social media vragen op over het gebruik van deze individuele en meestal openbare communicatiekanalen.

Uitgangspunt is dat professionals zelf weten hoe zij hiermee verstandig omgaan. Het digitale gedrag op social media wijkt niet af van het real life gedrag binnen de school.

Toch zijn er in scholen verschillen in kennis en ervaringen met, en meer of minder enthousiasme over social media. Dit protocol heeft als doel de dialoog over het gebruik ervan op gang te brengen en een handreiking te bieden voor meer duidelijkheid in het grijze gebied tussen binnen- en buitenschools mediagebruik.

Onder social media verstaan we bijv. Twitter, Facebook, LinkedIn, Instagram, YouTube en de wat minder bekende varianten daarop.

Richtlijnen gebruik social media

(Waar nu 'de school' staat kan de naam van de eigen school ingevuld worden).

1. Medewerkers van de school delen kennis en andere waardevolle informatie.
2. Bij onderwijs onderwerpen maken medewerkers duidelijk of zij op persoonlijke titel of namens de school publiceren.
3. Medewerkers van de school publiceren geen vertrouwelijke informatie op social media.
4. Ga niet in discussie met een leerling of ouder op social media.
5. Schoolbestuurders, schoolleiders en leidinggevenden zijn altijd vertegenwoordiger van de school, ook als zij een privémening verkondigen. Bij twijfel niet publiceren.
6. Medewerkers van de school zijn persoonlijk verantwoordelijk voor wat zij publiceren.
7. Medewerkers van de school weten dat publicaties op social media altijd vindbaar zijn.
8. Bij twijfel over een publicatie of over de raakvlakken met de school zoeken medewerkers contact met hun leidinggevende.
9. De school zorgt ook digitaal voor een veilig klimaat en communiceert met medewerkers, leerlingen en ouders hoe zij dit doet.
10. De school legt vast welke maatregelen zij neemt bij digitale overtredingen van medewerkers, leerlingen en ouders en communiceert dit met deze doelgroepen.

Praktische voorbeelden

<u>Kennisdeling</u>
Bijv. via Twitter of in LinkedIn groepen kan onderwijspersoneel zich mengen in discussies over onderwijszaken. Dit kan op basis van persoonlijke ervaringen. Als een standpunt van de school of organisatie gepubliceerd wordt, vermeldt de schrijver dit.

<u>Verantwoordelijkheid</u>
Hoofdregel: het gedrag van leraren op bijv. Facebook, YouTube en Twitter wijkt niet af van wat in de klas of op school gebruikelijk is. Don'ts:
- Foto's of filmpjes op van leraren op vakantie of in beschonken toestand op een feest.
- Te populair taalgebruik en schuttingtaal.

Veiligheid

De school heeft een verantwoordelijkheid als het gaat om de veiligheid van onderwijspersoneel en leerlingen. Dat begint met duidelijke en gecommuniceerde normen en waarden en de handhaving daarvan, ook digitaal. Scholen moeten zich niet laten verrassen door incidenten. Zorg voor duidelijke

regels over: welke mediadragers zijn in de klas en op school toegestaan? Ben je als school betrokken in het grijze gebied tussen privé en school? Wanneer schakel je ouders in, en wanneer politie? Welke sancties hanteer je bij welke overtreding? Hoe ga je om met slachtoffers en hoe met pers?

Er is al veel materiaal op dit gebied. Bijvoorbeeld op arboportaal.nl, schoolenveiligheid.nl en scholen kunnen natuurlijk informatie en kennis delen over deze onderwerpen. Communiceer de regels en afspraken duidelijk met onderwijspersoneel, leerlingen en ouders.

Voorbeelden die voor onveiligheid kunnen zorgen:
Kleineren van leraren of leerlingen via YouTube filmpjes
Dreigtweets van leerlingen
Digitale seksuele intimidatie of beschuldiging ervan.

Achtergrondinformatie Bedenk dat…

- Het gebruik van social media ‘real time’ gebeurt. Een druk op de knop en jouw bericht staat direct online.
- Online informatie misschien wel eeuwig online staat. Het is niet altijd gemakkelijk om informatie naderhand te (laten) verwijderen. Bedenk dus goed hoe je wilt overkomen in tekst, beeld en geluid – en niet alleen voor dat ene moment. Werkgevers, leerlingen en ouders zoeken soms op google naar meer informatie.
- Het een ongeschreven regel is om eenmaal geplaatste berichten niet te verwijderen. Met een druk op de knop (real time) worden ook foute berichten online geplaatst. Probeer de eerste te zijn om je eigen fouten te corrigeren, zonder eerdere berichten per definitie te wijzigen of te verwijderen. Vermeld daarbij dat jij degene bent die het bericht wijzigt. Geef bij verwijdering een goede reden.
- Je ook rekening dient te houden met het wettelijk vastgelegde auteurs-, beeld- en citaatrecht. Het is verboden om zonder toestemming van de maker andermans werk te publiceren. Schending van deze wet levert je een boete op van honderden euro’s.
- Sociale omgangsvormen online net zo goed gelden als offline. Respecteer degene tot wie je je richt. Laster, beledigingen en obsceniteit zijn niet geoorloofd. De privacy van anderen wordt gerespecteerd. Dit geldt voor zowel schoolbesturen, directies, onderwijspersoneel als voor leerlingen.
- Je zoveel mogelijk inhoudelijk dient te reageren op stukken van anderen. Alleen je mening geven, zonder onderbouwing daarvan, vervuilt de discussie en zegt meer over de schrijver van de reactie dan over het stuk. Onthoud dat dit soort reacties ook in een zoekmachine naar boven kunnen komen.
- Social media soms als gevolg hebben dat er een grijs gebied ontstaat tussen privé en werk gerelateerde zaken. Wanneer je op een persoonlijke blog over je werk schrijft, kun je een disclaimer (zie voorbeeld onderaan het protocol) opnemen waarin staat dat dit blog jouw persoonlijke standpunt weergeeft en dat dit niet overeen hoeft te komen met het standpunt van de school.

14.3.2 Modelreglement voor leerlingen

Dit model is bedoeld om het gesprek over het gedrag van leerlingen op school te stimuleren. Deze teksten dienen als inspiratie, maar kunnen ook integraal worden overgenomen. Het modelreglement is breed opgesteld. Deze versie kan ook van toepassing worden verklaard op onderwijzend en onderwijsondersteunend personeel. Dit kan door in artikel 1 toe te voegen dat het reglement van toepassing is op leraren/docenten en onderwijsondersteunend personeel van de school.

In het modelreglement zijn optionele teksten of varianten van teksten (gebaseerd op het type school) geel gearceerd.

Inleiding

Sociale media spelen een belangrijke rol in het leven van leerlingen en onderwijzend personeel. Het gebruik van sociale media is onderdeel van het gedrag van leerlingen binnen de school. Sociale media kunnen helpen om het onderwijs te verbeteren en de lessen leuker te maken, om contact te houden met vrienden, te experimenteren en grenzen te verleggen. Maar sociale media brengen ook risico's met zich mee, zoals pesten en het ongewild delen van foto's of andere gegevens.
Met dit reglement kan het gesprek op school, in de klas maar ook thuis gevoerd worden over wat er acceptabel is op sociale media (en wat niet). De afspraken zijn van toepassing op alle leerlingen van SCHOOL, voor het gebruik van sociale media op mobiele telefoons en andere (mobiele) devices. Niet alleen op school en in de klas, maar ook in het mediagebruik buiten de school.

Onder het gebruik van sociale media verstaan we het gebruik van programma's waarmee online informatie kan worden opgezocht, gedeeld en gepresenteerd. Denk bijvoorbeeld aan Facebook, Twitter, Instagram, YouTube, Snapchat maar ook alle (nieuwe) hiermee vergelijke programma's en apps.

Afspraken bij het gebruik van internet en sociale media

1. Dit reglement is van toepassing op alle leerlingen van SCHOOL, onafhankelijk van de plaats waar zij hun sociale media gebruiken.
2. We behandelen elkaar netjes en met respect, en laten iedereen in zijn waarde. Daarom pesten, kwetsen, stalken, bedreigen, beschadigen we elkaar niet en maken we elkaar niet zwart.
3. Iedereen is verantwoordelijk voor wat hij/zij zelf plaatst op sociale media, en kan daarop aangesproken worden. Ook het doorsturen (*forwarden*) en herplaatsen (*retweeten*) zijn handelingen waar je op aangesproken kunt worden.
4. Zorg dat je weet hoe de sociale media werken voordat je ze gebruikt, zorg dat de instellingen goed staan en je niet meer informatie deelt dan je wilt. Alles wat wordt gecommuniceerd via internet en sociale media blijft nog lang vindbaar.
5. Bij het gebruik van internet en sociale media houden we rekening met de goede naam van SCHOOL en iedereen die daarbij betrokken is zoals docenten, onderwijsondersteunend personeel en ouders.

6. We helpen elkaar om goed en verstandig met sociale media om te gaan en we spreken elkaar daarop aan. Als dat niet lukt, dan vragen we daarvoor hulp aan onze [leraar/mentor, afdelingscoördinator of directeur].
7. [De leerkracht moet vooraf toestemming geven om een mobiele telefoon of sociale media in de les te gebruiken. Tijdens examens, toetsen, overhoringen en proefwerken gelden aangepaste regels.]
   of:
   [Het meenemen van mobiele telefoon en daarmee vergelijkbare communicatieapparatuur op school is niet toegestaan. Een leerkracht kan in verband met het leerproces leerlingen toestemming geven om een mobiele telefoon mee te nemen en te gebruiken in de klas.]
   of:
   [Het gebruik van internet en sociale media is alleen toegestaan in de openbare ruimtes van de SCHOOL zoals de teamkamer, gangen en garderobe. Tijdens schoolactiviteiten zoals excursies is het gebruik van internet en sociale media alleen toegestaan tijdens de heen- en terugreis.]
8. We respecteren elkaars privacy. Bij het gebruik van internet en sociale media worden er daarom geen informatie, foto's of video's verspreid over anderen, als zij daar geen toestemming voor hebben gegeven, of als zij daar negatieve gevolgen van kunnen ondervinden.
9. Internet en sociale media worden alleen gebruikt voor acceptabele doeleinden. Het is daarom niet toegestaan om op school:
   a. sites te bezoeken of informatie te downloaden en te verspreiden die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend zijn;
   b. hacken en ongeoorloofd toegang te krijgen tot niet-openbare sites of programma's;
   c. informatie, foto's of video's te delen waarvan duidelijk is dat die niet bedoeld zijn om verder te verspreiden. Hou je wachtwoorden geheim;
   d. verzonnen berichten versturen of een fictieve naam gebruiken als afzender;
   e. iemand lastig vallen, te achtervolgen of te 'flamen'.
   f. Als iemand over de voorgaande punten informatie krijgt aangeboden, wordt dat gemeld aan de [leraar/mentor] of de [directeur/rector].
10. [Als er gebruikt wordt gemaakt van internet en sociale media via het netwerk van de school, dan mag dat de kwaliteit van het (draadloze) netwerk niet in gevaar brengen of schade aan personen of instellingen veroorzaken. Het hacken, overmatig downloaden of overbelasten van het netwerk is natuurlijk verboden.]

    [Leerlingen en medewerkers van SCHOOL worden geen 'vrienden' met elkaar op sociale media, tenzij het gaat om een door de medewerkers gebruikt professioneel account (waar geen persoonlijke informatie over de medewerker op is geplaatst).]
11. Als er geconstateerd wordt dat de afspraken niet worden nageleefd, wordt dit eerst met de betrokkene besproken. Bij een ernstige overtreding kan de directie van SCHOOL besluiten een maatregel op te leggen, die kan bestaan uit het in beslag nemen van de telefoon (of vergelijkbare communicatieapparatuur), [het uitsluiten van toegang tot het netwerk van de school], het geven van een disciplinaire maatregel (straf) of in het uiterste geval het schorsen of verwijderen van de leerling van school. Hierbij wordt er altijd contact opgenomen met de ouders van de leerling. Daarnaast kan de directie contact opnemen met de politie indien er sprake is van een strafbaar feit.

14.4 Format informatie ouders voor toestemming gebruik beeldmateriaal

[Plaats], [maand] [jaar]

Beste ouder/verzorger,

Op onze school laten wij u met beeldmateriaal (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 dit beeldmateriaal te zien zijn.

Wij gaan zorgvuldig om met deze foto's en video's. Wij plaatsen geen beeldmateriaal waardoor leerlingen schade kunnen ondervinden. We plaatsen bij foto's en video's geen namen van leerlingen. Daarnaast zijn wij vanuit de wetgeving verplicht om uw toestemming te vragen voor het gebruik van beeldmateriaal van uw zoon/dochter als hij/zij jonger is dan 16 jaar.
Leerlingen van 16 jaar en ouder moeten zelf toestemming geven.

Het is goed om het geven van toestemming samen met uw zoon/dochter te bespreken. Als u uw keuze thuis bespreekt, dan weten ze zelf waarom het gebruik van foto's en video's wel of niet mag. Het is goed mogelijk dat u niet wilt dat foto's van uw kind op internet verschijnen.

Uw toestemming geldt alleen voor beeldmateriaal dat door ons of in onze opdracht wordt gemaakt. Het kan voorkomen dat andere ouders foto's maken tijdens schoolactiviteiten. De school heeft daar geen invloed op, maar wij vertrouwen erop dat deze ouders ook terughoudend zijn met het plaatsen en delen van beeldmateriaal op internet. Bij het gebruik van internet en sociale media houden we rekening met de goede naam van SCHOOL en iedereen die daarbij betrokken is zoals docenten, onderwijsondersteunend personeel en ouders.

Met deze brief vragen we u aan te geven waarvoor [SCHOOL] **beeldmateriaal van uw zoon/dochter mag gebruiken.**
Op het toestemmingsformulier kunt u zien voor welk doel de verschillende opties gebruikt worden.

Als we beeldmateriaal willen laten maken voor onderzoeksdoeleinden, bijvoorbeeld om een les van een stagiair(e) 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, dan op het antwoordformulier vermeld staat, nemen we contact met u op.

U mag natuurlijk altijd de door u gegeven toestemming intrekken. Ook mag u op een later moment alsnog toestemming geven. Zonder toestemming zal er geen beeldmateriaal van uw zoon/dochter gebruikt en gedeeld worden.

Wilt uw het antwoordformulier met uw kind meegeven naar school?

Alvast bedankt voor uw medewerking!

Met vriendelijke groet,
[naam ondertekenaar]

14.5 Formulier toestemming gebruik beeldmateriaal en social media

Formulier toestemming gebruik beeldmateriaal en sociale media Schoolnaam
*gebruik eigen briefhoofd

TOESTEMMING GEBRUIK BEELDMATERIAAL	
Beeldmateriaal wordt gebruikt voor de volgende doelen: *(Aankruisen indien van toepassing*).	
In de schoolgids en/of schoolbrochure	☐ Informeren van (toekomstige) ouders en (toekomstige) leerlingen over de school en de onderwijs mogelijkheden. Hiernaast wordt het beeldmateriaal gebruikt voor PR-doeleinden van de school.
Op de openbare website van de school	☐ Informeren van (toekomstige) ouders en (toekomstige) leerlingen over de school, het gegeven en te volgen onderwijs en diverse onderwijsactiviteiten zoals schoolreisjes, schoolfeesten, etc.
In de (digitale) nieuwsbrief	☐ Ouders en leerlingen informeren over activiteiten en ontwikkelingen op en rondom school
Op sociale-media accounts van de school (Bijv. Twitter, Facebook)	☐ Informatie verspreiden over activiteiten (zoals schoolreisjes) en ontwikkelingen op school. Het delen van beeldmateriaal geeft een indruk over het gegeven onderwijs op school.
In het ouderportaal/app	☐ Informeren van ouders en leerlingen over de onderwijsactiviteiten zoals schoolreisjes, excursies, schoolfeesten, etc. Ouders en leerlingen informeren over activiteiten en ontwikkelingen op en rondom school.

Klassenfoto	☐ Mijn kind mag op de klassenfoto, gemaakt door de school zelf of door de schoolfotograaf (toestemming individuele foto's gaat via schoolfotograaf).

TOESTEMMING GEBRUIK SOCIALE MEDIA	
Sociale-media (Bijv.Twitter, Facebook)	☐ Ik ga ermee akkoord dat mijn kind tijdens de les onder toezicht van de leerkracht gebruik maakt van sociale media.

TOESTEMMING voor het maken van beeld- en geluidsopnames door studenten/stagiaires	
De afspraken zijn vastgelegd in de "Regeling Gezamenlijke verwerkingsverantwoordelijkheid beeldmateriaal" tussen Kerobei en bovenstaande opleidingsinstituten en is verkrijgbaar via de school van uw kind.	☐ Ik ga ermee akkoord dat studenten van HKE Fontys Venlo, Hogeschool De Kempel, Gilde Opleidingen en Vista College beeld- en geluidsopnames maken, uitsluitend bedoeld voor coaching en begeleiding en deze zijn alleen in te zien door de student en de coach. De opnames worden bewaard tot het gestelde doel bereikt is of de uitslag van het tentamen of examen bekend is, maar, bij gegronde redenen, uiterlijk tot het einde van het studiejaar waarin de beeld-en/of geluidsopnames gemaakt zijn.

TOEGANG PERSOONSGEGEVENS
☐ Indien ik op school onbedoeld in aanraking kom met persoonsgegevens van anderen zal ik hier zorgvuldig mee omgaan en dit meteen melden bij de directeur van de school.

INTREKKING TOESTEMMING GEBRUIK SOCIALE MEDIA EN BEELDMATERIAAL
☐ Ik ben ervan op de hoogte dat ouders/verzorgers te allen tijde en zonder opgaaf van redenen de toestemming m.b.t. het gebruik van sociale media en beeldmateriaal kunnen intrekken. Dit dient schriftelijk te gebeuren middels het formulier *Toestemming gebruik beeldmateriaal en sociale media*, voorzien van naam, datum en handtekening, verkrijgbaar bij de administratie van de school.
☐ **Ik ben op de hoogte van mijn rechten zoals vermeld in de privacyverklaring van Kerobei:** https://www.kerobei.nl/organisatie/kerobei-en-privacy

Hierbij verklaart ondergetekende dat alle in dit formulier aangevinkte items van toepassing zijn.	
Datum	
Naam ouder/verzorger	
Naam kind	
Groep	
Handtekening ouder/verzorger	
Ouder/verzorger 2 (wettelijk niet vereist, ter beoordeling van de school i.o.m. ouder(s)	
Datum	
Naam ouder/verzorger	
Handtekening ouder/verzorger	

14.6 Toelichting t.b.v. de school voor gebruik formulier toestemming gebruik beeldmateriaal en sociale media

In het toestemmingsformulier is aparte toestemming opgenomen voor verschillende categorieën. De wetgever eist dat een ouder een goed geïnformeerde 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 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.

Er is geen toestemming van ouders nodig voor het gebruik van beeldmateriaal 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 beeldmateriaal van leerlingen).

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 stellen zoals de (extreme) regel dat fotograferen van leerlingen tijdens de les of in klas alleen is toegestaan door docenten.

Als er beeldmateriaal op het beveiligde deel van de website door ouders gekopieerd wordt en vervolgens gedeeld via sociale media is dat niet meer de verantwoordelijkheid van de school. De school doet er wel goed aan om dit bij ouders onder de aandacht te brengen en hen te wijzen op hun verantwoordelijkheid hierin, bijv. via de schoolgids.

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.

14.7 Toestemmingsformulier beeld- en geluidsopnames door studenten/stagiaires

Toestemmingsformulier beeld- en geluidsopnames door studenten/stagiaires:

Beste ouder(s), verzorger(s)
Studenten van HKE Fontys Venlo, Hogeschool De Kempel, Gilde Opleidingen en Vista College lopen regelmatig stage op de school van uw kind. Er worden enkele beeldopnames gemaakt van hun activiteiten met leerlingen, onder de voorwaarden:
-Alle ouders van de betrokken leerling(en) hebben toestemming gegeven middels dit formulier.
-De opnames worden alleen gemaakt als dit noodzakelijk is voor coaching/begeleiding van de student/stagiair.
-De opnames worden veilig bewaard en zijn alleen toegankelijk voor de betrokken studenten en hun begeleiders.
-De opnames worden bewaard tot het gestelde doel bereikt is of de uitslag van het tentamen of

examen bekend is, maar, bij gegronde redenen, uiterlijk tot het einde van het studiejaar waarin de beeld-en/of geluidsopnames gemaakt zijn..

De afspraken zijn vastgelegd in de “Regeling Gezamenlijke verwerkingsverantwoordelijkheid beeldmateriaal” tussen Kerobei en bovenstaande opleidingsinstituten en is desgewenst verkrijgbaar via de school van uw kind.

Hierbij verleen ik toestemming voor het maken van beeld- en geluidsopnames door studenten/stagiaires van HKE Fontys Venlo, Hogeschool De Kempel, Gilde Opleidingen en Vista College.	
Ouder/verzorger van (naam leerling)	
Groep:	
Datum:	
Handtekening:	
Eventueel opmerking:	

De school is verplicht toestemming te vragen in het kader van de Algemene Verordening Gegevensbescherming (AVG). U kunt te allen tijde, zonder opgaaf van redenen, de toestemming intrekken.

14.8 Additionele informatie t..v. de school omtrent gebruik beeldmateriaal

14.8.1 Ouders of pers die foto’s en video’s maken

Als school ben je alleen verantwoordelijk voor foto’s die je zelf of in opdracht laat maken. Je bent dus niet verantwoordelijk voor de foto’s die een ouder tijdens een schoolreisje maakt en deelt via Facebook. Of de foto’s die een journalist maakt op het schoolplein. Dat betekent niet dat je als school niet hoeft op te treden. Weet je dat er leerlingen zijn die niet op de foto mogen? Hou ze dan weg bij de journalist. En vraag ouders om terughoudend te zijn met het delen van foto’s en bijvoorbeeld de leukste foto’s naar de leraar te sturen. De leraar kan dan zelf foto’s selecteren en foto’s verwijderen van leerlingen waarvan ouders geen toestemming hebben gegeven.

Zie: https://www.nvj.nl/privacy/avg/avg-en-journalistiek

14.8.2 Foto's van medewerkers

Wil je niet alleen de naam, maar ook foto's van de directie of leraren publiceren op de website van de school? Dan gelden er andere regels dan bij foto's van leerlingen. Met het publiceren van foto's van medewerkers laat je leerlingen en ouders zien wie er op school werkt. Zo maak je het contact met medewerkers persoonlijker en leerlingen kunnen hun leraar sneller herkennen. Omdat je zou kunnen zeggen dat de leraar, mentor, decaan of directielid zijn werk niet goed kan doen als zijn naam en foto niet bekend mag zijn, hoef je geen toestemming te vragen voor het plaatsen van de foto. In dit geval is de grondslag de (wettelijke) basis waarop je persoonsgegevens verwerkt.
Er zijn 6 mogelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
Je moet je medewerkers wel informeren dat je hun foto's publiceert. Ze kunnen dan eventueel – onderbouwd – bezwaar maken tegen de publicatie. Bijvoorbeeld in het geval van een problematische familiesituatie. Weeg daarom goed af welke foto's en persoonsgegevens je van je medewerkers deelt en waar ze neerzet. Misschien is het niet nodig om alle foto's op de publieke website te zetten, maar zorg je dat ze wel te zien via bijvoorbeeld het ouderportaal/app.

14.8.3 Uitzondering: foto's ter identificatie

Foto's gebruiken zonder toestemming mag niet. Er is hierop één uitzondering: het gebruik van een pasfoto voor identificatie. Hiervoor heeft een school een zogeheten 'gerechtvaardigd belang' om een foto te gebruiken. Het is voor school belangrijk om altijd een leerling te kunnen identificeren. Dit betekent dat je zonder toestemming pasfoto's van leerlingen mag gebruiken voor het leerling administratiesysteem of voor op een schoolpas.

14.8.4 Gebruik van foto's bij activiteiten in de klas

Wordt er in de klas bijv. een moederdag cadeautje geknutseld met een pasfoto? Of is een klas tijdens de tekenles bezig met een zelfportret aan de hand van een foto? Dan is er geen toestemming nodig voor het gebruik van de foto's. Wil je de zelfportretten met de bijbehorende pasfoto's op Facebook zetten? Dan is er wél toestemming nodig.

14.8.5 Toestemming door 1 of 2 ouders?

Zijn leerlingen jonger dan 16 jaar? Dan moeten ouders toestemming geven voor het gebruik van beeldmateriaal. Voor de wet is toestemming van één van beide ouders voldoende. Weet je als school dat de andere ouder liever geen toestemming geeft? Dan moet je van beide ouders toestemming hebben om foto's van de leerling te kunnen gebruiken. Voor het intrekken van de toestemming is de mededeling van één ouder genoeg. Vraag bij twijfel echter altijd om twee handtekeningen of gebruik de foto voor de zekerheid niet.

14.8.6 Klassenfoto

Voor het maken van een klassenfoto heb je altijd toestemming nodig van de leerlingen die erop komen. Vraag leerlingen of ouders dus altijd toestemming voor het maken en delen van de klassenfoto via je

toestemmingsformulier. Heb je van een leerling geen toestemming voor de klassenfoto? Dan gaat hij of zij dus niet op de foto.

14.8.7 Beeld- en geluidsmateriaal door student, stagiair of leraar binnen de school

Wil een student, stagiair of leraar video-opnames maken in de klas voor zijn of haar opleiding? En wordt dit materiaal alleen **binnen** de school gebruikt om de vaardigheden van de stagiair of leraar te beoordelen of evalueren? Dan is er voor de beelden geen toestemming nodig. Het is wel verstandig om de ouders of verzorgers van de leerlingen te melden dat er opnames worden gemaakt die alleen voor intern gebruik zijn. Hou daarnaast rekening met de volgende zaken:

Zorg dat de beelden veilig worden opgeslagen en bewaard. Verwijder de beelden als ze niet meer nodig zijn. Deel en publiceer de beelden niet. Hou als vuistregel aan dat de beelden de school niet mogen verlaten.

14.8.8 Beeld- en geluidsmateriaal door student, stagiair of leraar buiten de school

Het betreft hier opnamen die niet binnen de school blijven, maar bijv. op het opleidingsinstituut gebruikt worden. Hiervoor moet apart toestemming worden verleend door alle betrokken ouders. Dit is een taak van de school zie hfst.**14.7** voor het toestemmingsformulier.
Er is een Regeling Gezamenlijke Verwerkingsverantwoordelijkheid beeldmateriaal getroffen tussen CvB Kerobei en de betrokken opleidingsinstituten waarin o.a. duidelijk vermeld staat wie (mede)verantwoordelijk is, wat de verwerkingsdoelen zijn, welke persoonsgegevens verwerkt worden en wat de bewaartermijn is. De overeenkomst is ondertekend te worden door het bevoegd gezag van beide partijen. Het betreft HKE Fontys Venlo, Hogeschool De Kempel in Helmond, Gilde Opleidingen Venlo en Vista college. Studenten van evt andere opleidingen maken geen beeld- en geluidsopnames. De regelingen zijn in te zien in de gedeelde drive *BK – AVG – Kerobei en privacy.*

14.8.9 Video-oplossingen voor zieke leerlingen.

Een leerling is ziek thuis, maar wil toch zo veel mogelijk proberen om les te blijven volgen. Mag je de les in zo'n geval filmen of livestreamen? Privacy is hier mogelijk in het geding, omdat de zieke leerling, leraar en soms leerlingen in beeld komen.
Maak je gebruik van een livestream? Dan is het vragen van toestemming niet nodig. De zieke leerling ziet beelden die hij anders in de klas ook had gezien. Omdat de beelden niet opgenomen worden, is de kans op misbruik veel kleiner. Je bespreekt met de leraar, zieke leerling en zijn ouders dat je een livestream gebruikt en wat de regels daarvoor zijn. Je spreekt af met de leverancier dat de beelden niet worden opgenomen of bewaard en dat de verbinding goed wordt beveiligd. Informeer ouders van andere leerlingen in de klas, want hun kinderen kunnen wel in beeld komen.
Maak je een opname van de les? Dan is toestemming van leerlingen en/of ouders wel nodig, omdat het risico op misbruik van de beelden groter is. Zorg dat je ouders en leerlingen informeert over de opnames en wat er precies mee gebeurt. Van de leraar is geen toestemming nodig, maar je mag de beelden niet gebruiken om bijvoorbeeld de leraar te beoordelen. Verder maak je met de leraar, leerling en zijn ouders afspraken over wat er wel en niet mag gedaan worden met de opnames.

14.8.10 Schoolfotograaf

De schoolfotograaf krijgt foto's van leerlingen. Dat zijn persoonsgegevens. Soms krijgt de schoolfotograaf ook adressen van ouders om de foto's te verspreiden. Omdat de school de fotograaf persoonsgegevens ter beschikking stelt voor het uitvoeren van de werkzaamheden, moet de school een verwerkersovereenkomst afsluiten met de fotograaf. Dat zijn slechts een paar persoonsgegevens zoals NAW-gegevens van de ouders, de klas, enzovoort.

Schoolfotografen kunnen **de algemene verwerkersovereenkomst** van het privacy convenant gebruiken. Zo wordt het makkelijker om afspraken te maken met elkaar. Deze overeenkomst is speciaal voor leveranciers die wel verwerker zijn, maar geen digitale leermiddelen leveren.

De verwerkersovereenkomst biedt de school mogelijkheden om de schoolfotograaf beperkingen op te leggen over wat er wel en niet mag gebeuren met die gegevens en foto's.
Er zijn verschillende manieren waarop een school een schoolfotograaf in kan schakelen om foto's te laten verspreiden:

- de foto's kunnen in een envelop meegegeven worden aan de leerling
- de leerling krijgt een kaart met codes waarmee ouders thuis kunnen inloggen om de foto's te bekijken en bestellen
- de fotograaf stuurt de foto's en/of code op aan de ouders aan het adres dat de school aan de schoolfotograaf heeft verstrekt.

In alle gevallen maakt de school afspraken met de schoolfotograaf over de aflevering. De ouders verwachten dat ook, omdat zij niet betrokken zijn bij de afspraken met de schoolfotograaf. Er worden immers in opdracht van de school en onder schooltijd foto's gemaakt.
Voor de **klassenfoto** geldt dat de ouders voor het maken daarvan toestemming moeten geven, omdat hun kind op de klassenfoto wordt gezet die wordt verspreid en gedeeld met andere ouders. Zie **14.5**

De algemene verwerkersovereenkomst is te vinden via dit adres:
https://www.privacyconvenant.nl/algemene-verwerkersovereenkomst-onderwijs

14.8.11 Cameratoezicht

Er zijn 3 scholen met cameratoezicht rondom het gebouw, De Hazenkamp, Bösdael en Natuurlijk!
Momenteel vindt inventarisatie plaats van de voorwaarden en afspraken.

14.8.12 Intrekking toestemming gebruik beeldmateriaal en sociale media

Ouders hebben te allen tijde het recht om de toestemming voor het gebruik van beeldmateriaal wijzigen of in te trekken. Dit dient dit schriftelijk te gebeuren middels het formulier *Toestemming gebruik beeldmateriaal en sociale media*, voorzien van naam, datum en handtekening van beide ouders/verzorgers. Dit formulier is verkrijgbaar bij de administratie- of via het info-adres van de school.

Voorbeeldtekst voor opname schoolgids / ouderapp

Rechten van ouders/verzorgers op het gebied van privacy.

Kerobei verwerkt van al haar leerlingen persoonsgegevens. Kerobei vindt een goede omgang met persoonsgegevens van groot belang en is zich bewust van de privacywetgeving.
Kerobei is verantwoordelijk voor het zorgvuldig omgaan met de persoonsgegevens van ouders/verzorgers en leerlingen. In de privacyverklaring wordt uitgelegd hoe met persoonsgegevens van ouders en leerlingen wordt omgegaan. Deze is te vinden op:
https://www.kerobei.nl/organisatie/kerobei-en-privacy
Bij de aanmelding is al dan niet toestemming verleend aan de school voor bijvoorbeeld het gebruik van sociale media en beeldmateriaal. Kerobei wil er op wijzen dat ouders/verzorgers te allen tijde en zonder opgaaf van redenen de verleende toestemming voor bijvoorbeeld het gebruik van sociale media en beeldmateriaal kunnen intrekken. Dit dient schriftelijk te gebeuren middels het formulier *intrekking toestemming gebruik beeldmateriaal en sociale media*, voorzien van naam, datum en handtekening, verkrijgbaar bij de administratie van de school.

Formulier intrekking toestemming gebruik beeldmateriaal en sociale media Schoolnaam

INTREKKING TOESTEMMING GEBRUIK BEELDMATERIAAL	
Aankruisen indien van toepassing.	
In de schoolgids en/of schoolbrochure	☐ **INTREKKING TOESTEMMING** voor onderstaande: Informeren van (toekomstige) ouders en (toekomstige) leerlingen over de school en de onderwijs mogelijkheden. Hiernaast wordt het beeldmateriaal gebruikt voor PR-doeleinden van de school.
Op de openbare website van de school	☐ **INTREKKING TOESTEMMING** voor onderstaande: Informeren van (toekomstige) ouders en (toekomstige) leerlingen over de school, het gegeven en te volgen onderwijs en diverse onderwijsactiviteiten zoals schoolreisjes, schoolfeesten, etc.
In de (digitale) nieuwsbrief	☐ **INTREKKING TOESTEMMING** voor onderstaande: Ouders en leerlingen informeren over activiteiten en ontwikkelingen op en rondom school

Op sociale-media accounts van de school (Bijv. Twitter, Facebook)	☐ **INTREKKING TOESTEMMING** voor onderstaande: Informatie verspreiden over activiteiten (zoals schoolreisjes) en ontwikkelingen op school. Het delen van beeldmateriaal geeft een indruk over het gegeven onderwijs op school.
In het ouderportaal/app	☐ **INTREKKING TOESTEMMING** voor onderstaande: Informeren van ouders en leerlingen over de onderwijsactiviteiten zoals schoolreisjes, excursies, schoolfeesten, etc. Ouders en leerlingen informeren over activiteiten en ontwikkelingen op en rondom school.
Klassenfoto	☐ **INTREKKING TOESTEMMING** voor onderstaande: Mijn kind mag op de klassenfoto, gemaakt door de school zelf of door de schoolfotograaf (toestemming individuele foto's gaat via schoolfotograaf).

INTREKKING TOESTEMMING GEBRUIK SOCIALE MEDIA	
Sociale-media (Bijv.Twitter, Facebook)	☐ **INTREKKING TOESTEMMING** voor onderstaande: Ik ga ermee akkoord dat mijn kind tijdens de les onder toezicht van de leerkracht gebruik maakt van sociale media.

INTREKKING TOESTEMMING voor het maken van beeld- en geluidsopnames door studenten/stagiaires	
De afspraken zijn vastgelegd in de "Regeling Gezamenlijke verwerkingsverantwoordelijkheid beeldmateriaal" tussen Kerobei en bovenstaande opleidingsinstituten en is verkrijgbaar via de school van uw kind.	☐ **INTREKKING TOESTEMMING** voor onderstaande: Ik ga ermee akkoord dat studenten van HKE Fontys Venlo, Hogeschool De Kempel, Gilde Opleidingen en Vista College beeld- en geluidsopnames maken, uitsluitend bedoeld voor coaching en begeleiding en deze zijn alleen in te zien door de student en de coach. De opnames worden bewaard tot het gestelde doel bereikt is of de uitslag van het tentamen of examen bekend is, maar, bij gegronde redenen,

	uiterlijk tot het einde van het studiejaar waarin de beeld-en/of geluidsopnames gemaakt zijn.

☐ **Ik ben op de hoogte van mijn rechten zoals vermeld in de privacyverklaring van Kerobei:** https://www.kerobei.nl/organisatie/kerobei-en-privacy

Hierbij verklaart ondergetekende dat alle in dit formulier aangevinkte items van toepassing zijn.	
Datum	
Naam ouder/verzorger	
Naam kind	
Groep	
Handtekening ouder/verzorger	
Ouder/verzorger 2 (wettelijk niet vereist, ter beoordeling van de school i.o.m. ouder(s)	
Datum	
Naam ouder/verzorger	
Handtekening ouder/verzorger	

Zie ook **14.5** voor het toestemmingsformulier.

14.9 (Voor)aanmeldingsformulier Kerobei

Vanaf 14-11-22 gebruikt Kerobei een nieuw Vooraanmeldingsformulier waarin voortaan de toestemmingsverklaringen door ouders zelf ingevuld worden via het ouderportaal.
Afhankelijk van de samenstelling van de schoolpopulatie bepaalt iedere school of zij dit formulier gebruikt, óf dat het huidige formulier nog steeds leidend is.

Vooraanmeldingsformulier
Basisschool .....

*Doorhalen wat niet van toepassing is

GEGEVENS LEERLING

Achternaam .....

Voorvoegsel(s) .....

Voorna(a)m(en) .....

Roepnaam .....

Man / vrouw*

Geboortedatum ……

Geboorteplaats / geboorteland ……

Burgerservicenummer (BSN) ……

Huisartsenpraktijk ……

Eerste nationaliteit ……

Tweede nationaliteit ……

Datum in Nederland ……..

Straat / huisnummer ……..

Postcode / woonplaats……..……..Geheim: ja / nee*

Gezindte / godsdienst ……..……

Welke taal spreekt u met uw kind? Nederlands / dialect / anders* nl.……

GEZINSSITUATIE
Is er sprake van een éénoudergezin? ja / nee*

Namen broers en zussen met geboortedata
……
……

De gezinssituatie is als volgt geregeld:

- het gezag berust bij beide ouders gezamenlijk
- alleen moeder heeft het wettelijke gezag
- alleen vader heeft het wettelijke gezag
- anders, namelijk: ..……..……..……..

Heeft de rechter een van de ouders het recht van omgang met het kind ontzegd?

- nee
- ja, namelijk de moeder
- ja, namelijk de vader

Indien ja, graag een kopie van de gerechtelijke beslissing toevoegen

VOORSCHOOLSE PROGRAMMA'S

VVE indicatie (indien uw kind 3-4 dagdelen de peuterspeelzaal bezoekt)? ja / nee*

Naam peuterspeelzaal
……

Vanaf ……. - ……. - …….

Naam kinderdagverblijf……

Vanaf ……. - ……. - …….

ZIJ-INSTROMER (als uw kind al op een andere (basis)school gezeten heeft)

School en groep van herkomst
…….

Plaatsnaam school
……

Hoewel uw toestemming voor het opvragen van informatie bij de vorige school wettelijk niet verplicht is, willen we toch graag weten of u hiermee instemt:

- nee
- ja

MEDISCHE GEGEVENS (indien van toepassing)

Medicijnen
……
Allergisch voor
……..
Algemene medische gegevens
……..

Paramedische begeleiding (bijv. logopedie, fysiotherapie, ergotherapie)

- nee
- ja, namelijk (welke, wanneer) ……

Onderzoeken

Hebben er in het verleden onderzoeken plaatsgevonden met betrekking tot de (school)ontwikkeling van uw kind ?

- nee
- ja, namelijk (welk, wanneer)……..

Hebben er in het verleden onderzoeken plaatsgevonden naar, of heeft u hulp gehad bij het opvoeden en opgroeien van uw kind in uw gezin?

- nee
- ja, namelijk (vermeld ook het jaar of periode):…….

Ik geef hierbij toestemming om informatie op te vragen bij de volgende zorginstellingen of zorgverleners:

Naam organisatie:……

Eventuele contactpersoon:…….

Naam organisatie: ……..

Eventuele contactpersoon:…….

Naam organisatie: ……..

Eventuele contactpersoon: ……

TOESTEMMING GEBRUIK BEELDMATERIAAL EN SOCIALE MEDIA

De toestemmingen voor het gebruik van beeldmateriaal of andere zaken waarvoor uw toestemming nodig is, kunt u invullen in ons ouderportaal.
U ontvangt hier de informatie over als uw kind naar school komt.

GEGEVENS VERZORGERS

Eerste verzorger

wettelijke ouder / biologische ouder / voogd*

Man / vrouw*

Alleenstaand – gehuwd – samenwonend – geregistreerd partnerschap – gescheiden*

Achternaam en voorvoegsel(s) ……..

Roepnaam ……

Geboortedatum …….

Geboorteland ……

Nationaliteit(en) …….

Beroep …….

E-mailadres …….

Telefoon thuis ……..…….. Geheim: ja / nee*

Mobiele telefoon ……..…….. Geheim: ja / nee*

Telefoon werk ……..…….. Geheim: ja / nee*

Noodnummer, bij niet bereikbaarheid ouders ……

op naam van: …….

Tweede verzorger

wettelijke ouder / biologische ouder / voogd*

Man / vrouw*

Alleenstaand – gehuwd – samenwonend – geregistreerd partnerschap – gescheiden*

Achternaam en voorvoegsel(s) ……

Roepnaam …….

Geboortedatum …….

Geboorteland ……

Nationaliteit(en) ……

Beroep ……

Telefoon thuis ……Geheim: ja / nee*

Mobiele telefoon ……Geheim: ja / nee*

Telefoon werk ……Geheim: ja / nee*

E-mailadres ……..

Indien adres verzorger een/twee* afwijkt van leerling

Straat / huisnummer ……

Postcode / woonplaats .....Geheim: ja / nee*

VERKLARING
Met dit formulier doet u een vooraanmelding van uw kind op onze school.

Wanneer uw kind voor het eerst naar school gaat, ontvangt u circa 10 weken voordat uw kind 4 jaar wordt, een uitnodiging voor een intakegesprek. Na dit gesprek beslist de directie of uw kind definitief naar onze basisschool kan komen. Deze termijn van 10 weken geldt ook voor zij-instromers. Over deze beslissing krijgt u tijdig bericht.

De grondslag en de doelstellingen van de school worden door ons gerespecteerd en de hieruit voortvloeiende regels zullen door ons in acht worden genomen.

Ondergetekende verklaart dat dit formulier naar waarheid is ingevuld en op de hoogte is van de rechten zoals vermeld in de privacyverklaring van Kerobei. Deze verklaring is gepubliceerd op www.kerobei.nl. Bij het verwerken van de gegevens in dit aanmeldingsformulier houden wij ons aan de Algemene Verordening Gegevensbescherming (AVG).

Datum en handtekening eerste verzorger: Datum en handtekening tweede verzorger:

14.10 Gedragscode ICT-gebruik en privacy medewerkers Kerobei

Gedragscode privacy Kerobei.

De gedragscode t.a.v. privacy en veiligheid is opgenomen binnen de algemene gedragscode Kerobei onder het hoofdstuk “vertrouwelijkheid en privacy”

Kerobei communiceert op een professionele manier en handelt conform het informatiebeveiligings- en privacybeleid. Persoonsgegevens die door ons zijn verzameld, gebruiken we alleen voor het doel waarvoor ze verzameld zijn. Als we ze ook voor andere doeleinden willen verzamelen waar geen rechtsgrond voor is, vragen we opnieuw toestemming voor dat doel.

Ik doe het zo:
- Ik behandel vertrouwelijke informatie als zodanig;
- Ik zorg bij persoonlijke informatie over leerlingen, ouders en/of verzorgers of medewerkers voor voldoende privacy;
- Ik verstrek alleen gegevens aan personen en organisaties die hiertoe gerechtigd zijn;
- Ik sla gegevens op, op de daarvoor ingerichte en aangewezen ICT-systemen en/of fysieke bewaarplaatsen;
- Ik deel de persoonlijke wachtwoorden die door Kerobei zijn verstrekt niet met derden;
- Ik vergrendel mijn device als ik mijn werkplek verlaat;
- Ik onderhoud alleen schoolgerelateerde (online) contacten met leerlingen;

● Ik verstuur persoonsgegevens via een beveiligde verbinding (en niet via openbare wifi-netwerken);
● Ik ruim documenten met persoonsgegevens op voordat ik mijn werkplek verlaat;
● Ik print documenten met persoonsgegevens via beveiligd afdrukken;
● Ik meld gebeurtenissen en misstanden die te maken hebben met verwerking of toegang tot informatie bij mijn leidinggevende;
● Ik maak alleen gebruik van apps die binnen Kerobei zijn toegestaan (Kerobei app-checker);
● Ik gebruik de communicatiemiddelen van Kerobei alleen om informatie te delen over groeps- en schoolactiviteiten (en niet voor informatie over personen);
● Ik gebruik voor communicatie over groeps- of schoolactiviteiten alleen de e-mail, ouderportalen, social media- en overige accounts die door de school beheerd worden;
● Ik publiceer alleen foto's, video- of geluidsopnamen van leerlingen en collega's die hiervoor toestemming hebben gegeven.

Communicatie met derden

Binnen Kerobei wordt er, naast de fysieke contactmomenten, met ouders en andere betrokkenen buiten de school gecommuniceerd via e-mail, ParnasSys (inclusief ParnasSys-app), ouderportaal/app, de website, een nieuwsbrief en/of via sociale media. Het gebruik van digitale communicatiemiddelen sluit aan bij de eigentijdse manier waarop Kerobei betrokkenen wil informeren en toegankelijk wil zijn.
Kerobei stelt aan alle medewerkers een mailaccount beschikbaar en beheert accounts voor social media.
Van de medewerkers binnen Kerobei wordt verwacht dat zij:

- Genoemde publieke communicatiemiddelen, zoals website en social media, alleen inzetten om informatie te delen over groeps- en schoolactiviteiten (en geen informatie over personen).
- Voor communicatie over groeps- of schoolactiviteiten alleen gebruik maken van de e-mail-, ouderportalen, social media- en overige accounts die door de school beheerd worden.
- Alleen foto's, video- of geluidsopnamen van leerlingen en collega's publiceren die hiervoor (via de ouder/verzorger) expliciete toestemming hebben gegeven.

De medewerker heeft kennisgenomen van het *Privacyreglement Kerobei.* Alle items in dit document zijn van toepassing op deze gedragscode.

Wijzigingen in rechten (verandering van rol, taak, school enz.) worden doorgegeven via het daarvoor bestemde formulier ….
(Gedeelde drives\BK-Personeelsinformatie\Personeelszaken\Wijziging personeelsgegevens).

Voor akkoord en in tweevoud ondertekend:
De medewerker en de directeur bewaren ieder een exemplaar.

Medewerker	**Directeur**
Naam:	Naam:

Datum:	Datum:
Plaats:	Plaats:
Functie:	Directeur
Handtekening:	Handtekening:

14.11 Informatiebeveiligingsbeleid Kerobei

14.11.1 Data

Het hacken van software en netwerken kan nooit 100% uitgesloten worden, maar de kans wordt aanzienlijk verkleind als men bij een gerenommeerd, ISO gecertificeerd datacentrum is aangesloten. Cloudwise beheert ons netwerk en onze data op professionele wijze en wij vertrouwen als stichting op de expertise en beveiliging van dit bedrijf. Cloudwise is ISO gecertificeerd en dient zich te houden aan de 'ISO 27001 Informatiebeveiliging'. Zij voeren zelf voortdurend risicoanalyses uit en handelen dienovereenkomstig volgens de wet.

Data op het netwerk wordt afgeschermd door medewerkers een persoonlijk account te geven met voor hun toepasselijke rechten op de dataschijven. E.e.a. wordt afgedekt door identity-management middels Workspace en het COOL-Portaal van Cloudwise.

Vanaf oktober 2022 gebruiken voor Google for Workspace de licentie Educational Plus. Deze versie garandeert dataopslag binnen de Europese Unie i.v.m. EU privacy regels.

Via SIVON (landelijke samenwerking en inkoopcoöperatie schoolbesturen) maken we sinds januari 2022 gebruik van Veilig Internet.
Naast een internetverbinding met de juiste snelheid en betrouwbaarheid beschikken we over een professioneel beheerde firewall via het diensten centrum van OC & W.

Daarnaast gebruiken we vanaf augustus 2022 de licentie AFI backup Google Workspace waarmee we op bestandsniveau data kunnen terughalen.

Datamappen met bestanden waarin privacygevoelige of vertrouwelijke gegevens zijn op het stafbureau en de scholen van Kerobei alleen maar toegankelijk voor personeelsleden die expliciet toegang hebben verkregen tot deze datamappen.
Alle personeelsleden van Kerobei kunnen extern via elk apparaat toegang krijgen tot het webbased netwerk van Kerobei. Zij moeten daar met hun persoonlijke inloggegevens inloggen.
Door nieuwsberichten voor alle personeel van Kerobei en aandacht voor dit thema op de werkplaatsen (bijv. directeuren, ICT-ambassadeurs) blijven we inspanningen leveren om op het netvlies van

personeelsleden te houden, dat we veilig dienen om te gaan met data en privacygevoelige gegevens. De zwakste schakel is immers de mens zelf.

14.11.2 Gebruikers- en software beheer

Zoals eerder aangegeven hebben alle medewerkers een persoonlijk account met daaraan gekoppelde rechten voor toegang tot data, mail en softwarepakketten. Het aanmaken van een account kan door Cloudwise, de ICT-beheerder en administratieve medewerker van de school of door de manager IBP gedaan worden; het beheer ervan geschiedt op voornamelijk op schoolniveau. Bij calamiteiten kan door hiervoor genoemde partijen een account per direct geblokkeerd worden.
Door wisseling van rollen, taken of school is het belangrijk dat de rechten actueel zijn. Dit is een gezamenlijke verantwoordelijkheid van medewerker en directeur. Middels een wijzigingsformulier, beschikbaar op het intranet, kan een medewerker de wijzigingen doorgeven. Deze worden uitgevoerd door de ICT-beheerder van de school, de manager IBP of de beheerders van door Kerobei gebruikte softwarepakketten.
Bij beëindiging van het dienstverband wordt het account op de eerstvolgende werkdag volgend op de datum van uittreding ontoegankelijk gemaakt op last van de directeur.
Regelmatig worden onze medewerkers geattendeerd op het actueel houden van hun rechten, door nieuwsberichten, ICT-ambassadeurs en directeuren.
Voor leerlingen zijn de rechten standaard vastgesteld. Indien leerlingen in het administratiepakket worden uitgeschreven wordt het account, na synchronisatie, gewist.
Binnen Kerobei is het (nog) niet verplicht om regelmatig hun wachtwoord te wijzigen.
Er wordt wel over nagedacht omdat dit een mogelijk risico vormt.
Medewerkers die hun wachtwoord zijn vergeten kunnen dit via Cloudwise of de beheerder op school laten resetten; het tijdelijke wachtwoord wordt per mail verstuurd of mondeling overgebracht (niet per telefoon) waarna men een nieuw wachtwoord moet kiezen dat aan strenge voorwaarden moet voldoen.
Van medewerkers wordt verwacht dat zij hun computer vergrendelen als ze hun werkplek verlaten, dit om een datalek te voorkomen. Het verdient voortdurende aandacht van allen, om elkaar aan te spreken op “openstaande beeldschermen”!
Het leerling administratie- en volgsysteem (ParnasSys) bevat veel privacygevoelige informatie over leerlingen (en ouders). Dit is een webapplicatie die overal ter wereld te benaderen is. Het wachtwoord moet voldoen aan de strenge eisen die het pakket stelt (min 12 tekens). Ook heeft de applicatie de ingebouwde beveiliging dat mensen na 60 minuten inactiviteit worden uitgelogd.

De personeels- en salarisadministratie wordt gedaan in Merces HR2Day. De medewerkers die toegang hebben tot deze gegevens werken middels een eigen, voor hun werkzaamheden afgestemde, account. Alle andere medewerkers hebben alleen toegang in *HR2Day selfservice,* waarbij zij alleen voor hun toegankelijke en relevante informatie kunnen zien.

De veiligheid en toegang tot alle softwarepakketten wordt door de leveranciers bepaald. Voor alle pakketten is een verwerkersovereenkomst gemaakt of opgevraagd zodat de privacy van ‘onze’ leerlingen en medewerkers gewaarborgd is. De verwerkersovereenkomsten zijn voor alle medewerkers in te zien op het Intranet:
Gedeelde Drives\ BK - AVG - Kerobei en privacy\Verwerkersovereenkomsten

14.11.3 Beleid voor Apps en add-ons binnen Kerobei.

Voor deze toepassingen is extra aandacht nodig omdat met de makers meestal geen verwerkersovereenkomst kan worden afgesloten en Kerobei de veiligheid uiteraard toch wil garanderen.
Scholen voeren een wettelijke taak uit, namelijk het verzorgen van onderwijs. Kerobei wil dat onderwijs optimaal en in de huidige tijdgeest verzorgen en gebruikt daarvoor allerlei leermiddelen. Dat kunnen boeken zijn, maar ook digitale middelen, zoals apps en add-ons. Kerobei maakt gebruik van kernapplicaties in Workspace. Als het gaat om apps en meer geavanceerde functies is het Workspace pakket niet altijd toereikend. Om leerlingen op een bepaald gebied te helpen, maken leerkrachten soms gebruik van door derden ontwikkelde functionaliteiten. Dit kan een belangrijke extra ondersteuning voor de leerling opleveren. De school is er echter verantwoordelijk en aansprakelijk voor dat apps aan een aantal eisen t.a.v. privacy en veiligheid voldoen; een lijst met beoordelingen van apps en add-ons is inmiddels beschikbaar op de website Kerobei App checker Kerobei App-checker. De website is bereikbaar middels een tegel in het COOL-Portaal. De apps worden door functionaris gegevensbescherming beoordeeld met een groen- (veilig gebruik), oranje- (gebruik onder voorwaarden) of rood stoplicht (gebruik niet toegestaan). Op de Kerobei app-checker is bij het oranje stoplicht een toelichting beschikbaar of klik HIER.

Het doel van het beleid omtrent het gebruik van apps is
Het waarborgen van eigentijds en kwalitatief hoogstaand onderwijs, waar nodig gericht op de individuele leerling
Het waarborgen van een veilige leeromgeving voor betrokkenen, dus ook voor de leerkracht en rekening houdend met de eisen van de privacywetgeving (AVG) en de functionaliteit van de app(s)
Het voorkomen van privacy- en beveiligingsincidenten en het beperken van de mogelijke gevolgen daarvan.
Het beleid omtrent het gebruik van apps geldt voor alle medewerkers, leerlingen, ouders/verzorgers, bezoekers en externe relaties, alsmede alle devices waarmee geautoriseerde toegang tot het schoolnetwerk verkregen kan worden. Het beleid geldt voor alle apps die aangeboden worden door de school en derhalve onder de verantwoordelijkheid van de school vallen.
Uitgangspunt van Kerobei is dat professionals zelf bepalen welke tools zij inzetten, maar om te helpen om die veilig en met inachtneming van de privacywetgeving in te zetten, heeft Kerobei de volgende richtlijnen en voorwaarden voor het gebruik van apps en add-ons opgesteld:
Apps en add-ons die niet tot de standaard tools in Workspace behoren, zijn niet altijd advertentievrij.
Houd er rekening mee dat een verwerkersovereenkomst met de leverancier van de app dan noodzakelijk is. Zie hiervoor de gedeelde drive:

BK - AVG - Kerobei en privacy.

Beperk het aantal apps dat je gebruikt. Er zijn heel veel mogelijkheden en leerlingen kunnen het overzicht verliezen en overal hetzelfde wachtwoord voor gaan gebruiken.

Kerobei verwacht van alle gebruikers van apps dat zij deze op een verantwoorde manier gebruikt en met name onveilige situaties, discriminatie en intimidatie vermijdt.

Datalekken en incidenten dienen op de afgesproken wijze te worden gemeld.

Uitvoering beoordeling nieuwe apps/add-ons:

Indien een medewerker een app/add-on wil gebruiken wordt is de volgorde van handeling:

1. Staat de app/add-on op de Kerobei app-checker?
2. Zo nee, is de app/add-on onderwijsinhoudelijk van goede kwaliteit?
3. Zijn er alternatieven in bestaande programma's (basispoort/Gynzy/Presenter enz) van aanbieders waarmee we een verwerkersovereenkomst hebben? (BK - AVG - Kerobei en privacy\Verwerkersovereenkomsten).
4. Is de app/add-on specifiek voor je klas, jezelf of ook geschikt voor gebruik binnen Kerobei?
5. Is de app/add-on gratis? Zo ja beoordeel dan eerst zelf globaal veiligheid/privacy.Privacy op School (https://www.privacyopschool.nl)
6. Overleg met de ICT-ambassadeur, die vervolgens per mail een beoordeling kan aanvragen bij de FG vanuit Privacy op School (https://www.privacyopschool.nl)
7. De indiener krijgt bericht terug van Theo met een cc naar jeroen.geurts@kerobei.nl die de app/add-on in de Kerobei app checker opneemt.

*de Fg vanuit Privacy op School (https://www.privacyopschool.nl) neemt alleen opdrachten aan van ICT-ambassadeurs. Dit om verdere wildgroei te voorkomen.

Kerobei streeft ernaar dat per 1-1-2022 alleen nog goedgekeurde apps worden gebruikt.
Dit betekent dat elke school de in gebruik zijnde apps controleert en het aantal minimaliseert.

14.11.4 Hardware

Hardware waarmee binnen de scholen en bestuurskantoor van Kerobei toegang wordt verkregen tot het netwerk van Kerobei moet worden gecertificeerd en geïnstalleerd door Cloudwise. Omdat het netwerk en alle hardware door Cloudwise op professionele wijze is geconfigureerd en up-to-date wordt gehouden, wordt de kans op hacken aanzienlijk verkleind. We verwachten van de medewerkers dat zij alleen inloggen op devices waarop een up-to-date virusscanner is geïnstalleerd en alleen gebruik maken van een beveiligde Internet- of WIFI-verbinding. Dit staat ook vermeld in onze gedragscode zie **14.10**.
Aangezien al onze data staat opgeslagen in Workspace is het fysiek beveiligen van onze computers in feite overbodig, aangezien er geen persoonsgegevens of bestanden op kunnen worden opgeslagen. Dit wordt door de installatie van Cloudwise onmogelijk gemaakt.
Bij een laptop of ander mobiel device wordt soms wel de harde schijf gebruikt, dus als deze wordt ontvreemd of verloren is er wél kans op een datalek. Kerobei adviseert om de lokale harde schijf alleen te gebruiken indien het niet anders kan, bijv. als er geen Internetverbinding beschikbaar is.
Zie ook de brochure van Kennisnet: Handreiking verantwoord gebruik bedrijfsmiddelen

14.11.5 Wat kan een medewerker doen om datalekken te voorkomen?

Iedere werknemer dient op de hoogte te zijn van de inhoud van de gedragscode ICT-gebruik en privacy medewerkers, zie bijlage **14.10.** Hierin staan alle richtlijnen omtrent dit onderwerp.

14.12 Model Responsible Disclosure voor medewerkers

Bij <naam school> vinden wij de veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Als jij een zwakke plek in één van onze systemen hebt gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met jou samenwerken om de leerlingen, medewerkers en onze systemen beter te kunnen beschermen.

Wij vragen jou:

Je bevindingen door te geven aan de directeur van de school, mondeling of via mail. De directeur bepaalt of er vervolgstappen nodig zijn en voert die i.o. m. jou uit.

De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of (persoons)gegevens van derden in te kijken, te verwijderen of aan te passen.

De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle (vertrouwelijke) gegevens die zijn verkregen via het lek direct na het verhelpen van het lek te wissen.

Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden.

Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wij zeggen toe dat:

Wij binnen 3 dagen reageren op je melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.

Als je je aan bovenstaande voorwaarden hebt gehouden zullen wij geen juridische stappen tegen jou ondernemen met betrekking tot de melding*.

Wij behandelen je melding vertrouwelijk en zullen je persoonlijke gegevens niet zonder jouw toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk.

Wij houden je op de hoogte van de voortgang van het verhelpen van de kwetsbaarheid.

In berichtgeving over het gemelde probleem zullen wij, indien je dit wenst, je naam vermelden als de ontdekker. Wij streven ernaar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

* Let op: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Er bestaat een kans dat je tijdens je onderzoek handelingen uitvoert die volgens het strafrecht strafbaar zijn. Het feit dat Kerobei geen aangifte tegen jou zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar je handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.

14.13 Model Responsible Disclosure voor leerlingen

Bij <naam school> vinden wij de veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Als jij een zwakke plek in één van onze

systemen hebt gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met jou samenwerken om de leerlingen, medewerkers en onze systemen beter te kunnen beschermen.

Wij vragen jou:
Je bevindingen door te geven aan je meester/juf.
De kwetsbaarheid niet te misbruiken.
De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle informatie die verkregen is via het lek direct na het verhelpen van het lek te wissen;
De school voldoende informatie te geven om het probleem te kunnen vinden.

Wij beloven dat:
Je binnen 3 dagen van ons te horen krijgt hoe we de kwetsbaarheid gaan oppakken en wanneer wij hiervoor een oplossing verwachten te hebben;
Als je de kwetsbaarheid netjes gemeld hebt en via de bovenstaande stappen gehandeld hebt, zullen wij geen melding maken bij de politie.
Wij jouw melding vertrouwelijk behandelen en dat jouw persoonlijke gegevens niet zonder jouw toestemming met anderen delen worden tenzij dit wettelijke verplicht is;
(Optioneel) Als je de kwetsbaarheid gemeld hebt volgens bovenstaande stappen, ontvang je van ons een passende beloning;
Wij je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid.

Let op: Alle gele onderdelen invullen op basis van de gegevens van de school.

14.14 Welke gegevens verwerkt Kerobei en rechten van ouders

Zie Privacyverklaring Kerobei: Kerobei en privacy

De tekst uit dit hoofdstuk is vervangen door privacyverklaring

14.15. Wettelijke informatieplicht aan ouders

Situatie	Alle informatie	Beperkte informatie i.o.m CvB	Geen inf. i.o.m CvB
Ouders die met elkaar getrouwd zijn en beide het gezag hebben.	Beide ouders. Zij bepalen welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).		
Ouders die getrouwd zijn waarvan één ouder het gezag heeft en één ouder het kind erkend heeft.	De ouder die gezag heeft. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).	De ouder die het kind erkend heeft, heeft recht op beperkte informatie waar hij/zij zelf om moet vragen. Het betreft alleen belangrijke feiten en omstandigheden dus informatie over schoolvorderingen en evt. sociaal-pedagogische ontwikkelingen op school tenzij de veiligheid van het kind niet gewaarborgd kan worden (bijv. signalen van kindermishandeling / huiselijk geweld)**	
Ouders die getrouwd zijn waarvan 1 ouder het gezag heeft en 1 ouder geen gezag heeft en zijn kind niet erkend heeft.	De ouder die gezag heeft. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).		De ouder die geen gezag heeft en het kind niet erkend heeft.
Ouders die getrouwd zijn waarvan beide ouders het gezag niet hebben maar wel hun kind erkend hebben. Er is een voogd toegewezen*.	De voogd. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. leefgroep, niet gezaghebbende ouder, pleegouders, grootouders).	De ouders hebben recht op beperkte informatie waar zij zelf om moet vragen. Het betreft alleen belangrijke feiten en omstandigheden dus informatie over schoolvorderingen en evt. sociaal-pedagogische ontwikkelingen op school tenzij de veiligheid van het kind niet gewaarborgd kan worden (bijv. signalen van kindermishandeling/huiselijk geweld)**	

Ouders die gescheiden zijn, waarvan beide ouders het gezag hebben.	Beide ouders. Zij bepalen welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).	Indien er signalen zijn van kindermishandeling/huiselijk geweld.	
Ouders die gescheiden zijn, waarvan 1 ouder het gezag heeft en 1 ouder het kind erkend heeft.	De ouder die gezag heeft. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).	De ouder die het kind erkend heeft, heeft recht op beperkte informatie waar hij/zij zelf om moet vragen. Het betreft alleen belangrijke feiten en omstandigheden dus informatie over schoolvorderingen en evt. sociaal-pedagogische ontwikkelingen op school tenzij de veiligheid van het kind niet gewaarborgd kan worden (bijv. signalen van kindermishandeling/ huiselijk geweld)**	
Ouders die gescheiden zijn, waarvan 1 ouder het gezag heeft en 1 ouder het kind niet erkend heeft.	De ouder die gezag heeft. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).		De ouder die geen gezag heeft en het kind niet erkend heeft.
Ouders die gescheiden zijn, waarvan beide ouders geen gezag hebben en het kind erkend hebben. Er is een voogdijmaatregel* uitgesproken door de rechter.	De voogd. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. leefgroep, niet gezaghebbende ouder, pleegouders, grootouders).	De ouders hebben recht op beperkte informatie waar zij zelf om moet vragen. Het betreft alleen belangrijke feiten en omstandigheden dus informatie over schoolvorderingen en evt. sociaal-pedagogische ontwikkelingen op school tenzij de veiligheid van het kind niet gewaarborgd kan worden (bijv. signalen van kindermishandeling/huiselijk geweld)**	

*In Nederland staan alle minderjarigen (kinderen onder de 18 jaar) onder gezag. Meestal hebben de ouders samen het gezag: het “ouderlijk gezag”. Het gezag kan ook worden uitgeoefend door een ouder en een niet-ouder samen (bijvoorbeeld de partner van een vader of moeder). Dit wordt “gezamenlijk gezag” genoemd.
Als ouders scheiden behouden zij in principe beiden het gezag over het kind. Als een ander dan de ouder(s) het gezag uitoefent wordt dit “voogdij” genoemd. De voogdijmaatregel wordt uitgesproken door de kinderrechter. Dit betekent dus ook dat de ouders geen gezag meer hebben.
Wanneer er een OTS (onder toezicht stelling) wordt uitgesproken door de kinderrechter betekent dit dat de ouders (of een van de ouders) nog steeds het ouderlijk gezag heeft, maar onder toezicht staan. Er wordt dan een gezinsvoogd toegewezen.

** Hierbij zijn twee uitzonderingen:

1. De informatie wordt niet verstrekt als de school de informatie niet op dezelfde manier aan de ouder met het ouderlijk gezag zou verstrekken;
2. De informatie wordt niet verstrekt als het belang van het kind zich tegen het verschaffen van de informatie verzet.

Voor meer info:
https://onderwijsgeschillen.nl/thema/informatieverstrekking-aan-gescheiden-ouders#wettelijke

14.16 Rechten van betrokkenen (ouders, leerlingen en evt. derden)

Recht op informatie houdt in dat de leerling en/of zijn ouders (de betrokkenen) vooraf in begrijpelijke taal actief en laagdrempelig worden geïnformeerd over welke gegevens met welk doel worden verwerkt en wat de rechten van de leerling zijn.

Procedure Inzagerecht

Ouders hebben het recht om de persoonsgegevens van hun kind die door de school worden verwerkt, in te zien. Hier hoeft geen reden voor te worden gegeven.
De school heeft één maand de tijd om te voldoen aan dit verzoek.
Zij mogen dit doen met redelijke tussenpozen.Het uitgangspunt is dat ouders het doel aangeven waarvoor zij deze vraag stellen.
Ouders hebben het recht om op hoofdlijnen te worden geïnformeerd over het gebruik van de gegevens van hun kind. De school is daarom niet verplicht om het hele dossier ter inzage te stellen.

Ouders kunnen een (gratis) kopie krijgen van de opgenomen persoonsgegevens. Er mag ook worden gekozen om de betrokkene ‘live’ inzage te geven in de systemen (de medewerker van de school is daarbij aanwezig). Als het inzageverzoek digitaal wordt ingediend, dan krijgt zij via die zelfde weg de informatie (digitale kopieën).

Als de school van mening is dat het verstrekken van bepaalde informatie aan de ouders in een bepaald geval het belang van het kind schaadt en kan leiden tot fysieke of mentale schade, dan kan de school in het uiterste geval beslissen om inzage te weigeren. Dat kan als dit noodzakelijk en evenredig is ter waarborging van bepaalde (in de AVG genoemde) belangen, waaronder de bescherming van de betrokkene of van de rechten/vrijheden van een ander. De school zal in zo’n geval een zorgvuldige belangenafweging moeten maken. Hierbij kan gedacht worden aan zaken waarop de meldcode huiselijk geweld en kindermishandeling ziet ; het verdient aanbeveling de overwegingen in het Afwegingskader bij de meldcode te lezen.

Wettelijke grondslag

-Inzage is een recht (AVG art. 15)
-Niet bedoeld om informatie te verzamelen voor een rechtszaak
-bedoeld om de rechtmatigheid van verwerking van de

gegevensverwerking te verifiëren

Kader

Uitgangspunt blijft wederzijds vertrouwen waardoor we handelen in de geest van de wet, en de grenzen alleen zoeken bij een conflict.

Denk hieraan:

- Er is altijd meer aan de hand
- De reden van de aanvraag is (vaak) niet bekend
- Aanvragers willen soms direct inzage
- Gesprekken nooit alleen
- Wees feitelijk, geen meningen
- Citeer, oberservaties zijn prima, mits verdedigbaar
- Een kopie van het héle dossier hoeft dus niet
- Geen kopiën van e-mails die al met de aanvrager zijn uitgewisseld

Recht op inzage in en correctie van de persoonsgegevens. De betrokkene heeft het recht op inzage van zijn gegevens en het verbeteren of aanvullen van ontbrekende of verkeerd vastgelegde persoonsgegevens.
Recht op verwijdering van de persoonsgegevens die niet (langer) nodig zijn om de vastgestelde doelen te behalen. Het gaat alleen om gegevens die niet noodzakelijk zijn, of als het opslaan van die gegevens in strijd is met de wet. Een leerling kan dus niet vragen om een onvoldoende beoordeling voor bijv. een toets te 'verwijderen' op grond van privacywetgeving.
Recht van verzet tegen verwerking van persoonsgegevens bij de grondslag gerechtvaardigd belang of verzet tegen direct marketing en profilering. De betrokkene kan verzet instellen tegen een verwerking van zijn persoonsgegevens die plaatsvond op grond van een gerechtvaardigd belang. De school maakt een afweging van het privacybelang van de leerling, tegenover het belang van de school om gegevens wél te gebruiken.
De leerling en/of zijn ouders hebben **het recht om bij toestemming**, ook een beperkte toestemming te geven of toestemming te onthouden voor een onderdeel van de verwerking (**granulaire toestemming**).
De leerling en/of zijn ouders hebben het **recht dat verbeteringen**, aanvullingen of verwijderingen aan alle andere partijen worden doorgegeven aan wie een organisatie de persoonsgegevens van betrokkene heeft verstrekt.
Het recht op 'bevriezing van de verwerking' van zijn gegevens
De betrokkene heeft het '**recht om te worden vergeten'** door het volledig wissen van de persoonsgegevens, tenzij er een wettelijke bewaarplicht geldt of het verwijderen in strijd is met de vrijheid van meningsuiting. Voor het onderwijs is dit recht minder relevant omdat er veel wettelijke bewaartermijnen gelden.
In geval van toestemming of een overeenkomst met de betrokkene, heeft de betrokkene het **recht op dataportabiliteit** als de verwerking van persoonsgegevens plaatsvindt op de grondslag toestemming. Scholen werken niet veel met toestemming, daarom is dit recht minder relevant.

Recht op melding datalek: bij een datalek hebben de leerling en/of zijn ouders recht om daarover geïnformeerd te worden indien zij daar een zwaarwegend belang bij hebben.

Voor meer informatie zie Handreiking rechten betrokkenen in het PO/VO op de site van Kennisnet.

14.17 Risicoanalyse

Een risico is een gebeurtenis die leidt tot een gevolg door een bepaalde oorzaak. Daarnaast heeft een risico ook een kans en een impact.

Kans op het optreden van een risico:

Klein:	minder dan jaarlijks (1 punt).
Middel:	meerdere keren per jaar (2 punten).
Groot:	kan dagelijks voorkomen (3 punten).

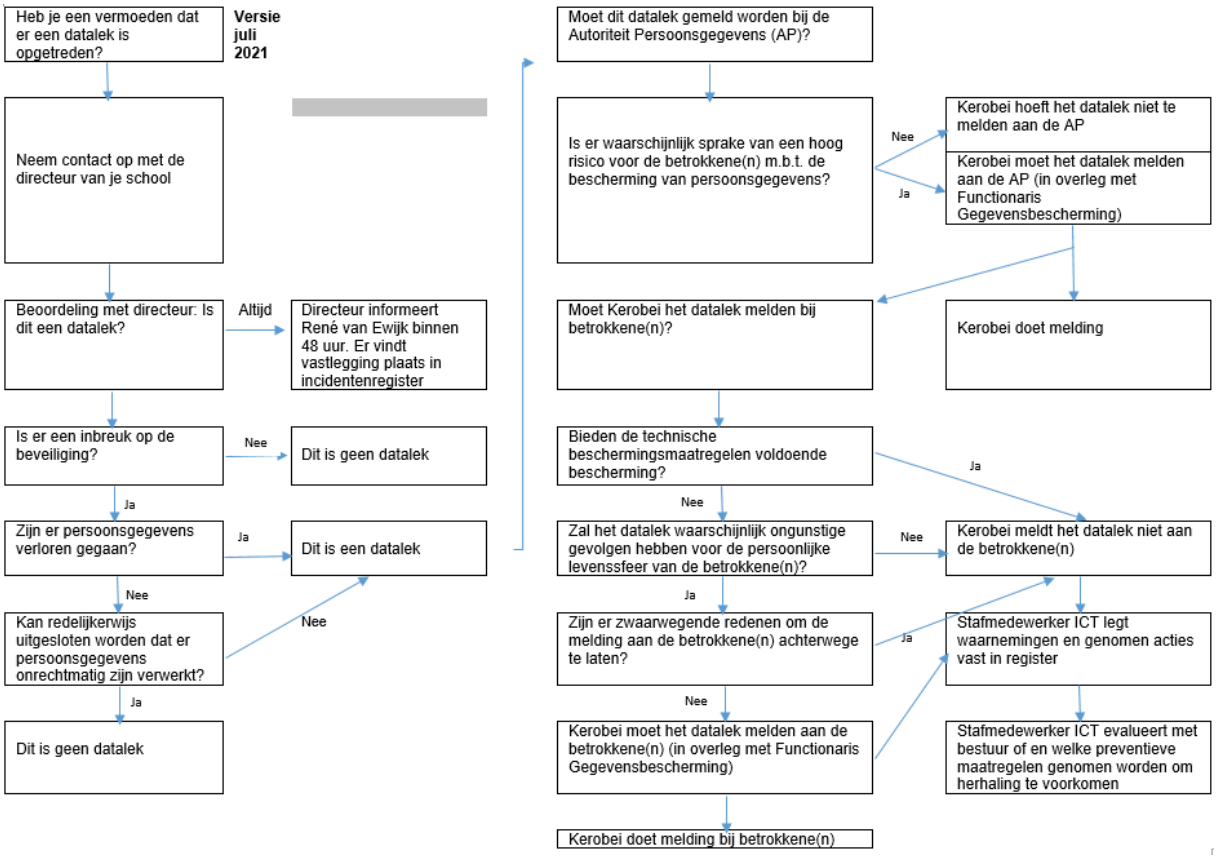
Impact effect als het risico waarheid wordt/nadelige gevolgen:

Klein:	verstoring niet-primair proces, alleen intern merkbaar (1 punt).
Middel:	verstoring primair proces, extern merkbaar snel opgelost (2 punten).
Groot:	verstoring primair proces, reputatieschade, langdurig (3 punten).

Kans x impact = risicoscore.

Categorie		Kan	Impac	Score
Mensen	Cultuur en discipline met autorisaties niet goed	3	3	9
Gegevens	Diefstal of zoekraken (bewust omgaan met privacy)	2	3	6
Mensen	Beeldmateriaal leerlingen gepubliceerd zonder toestemming	3	2	6
Apparatuur	Gegevens op printer laten liggen	3	2	6
Organisatie	Onduidelijke verantwoordelijkheden	3	2	6
Gegevens	Personeelsgegevens niet achter slot en grendel	3	2	6
Mensen	Onveilige passwords	2	2	4
Gegevens	Backup/recovery niet goed	1	3	3
Omgeving	Brand	1	3	3
Mensen	Leerlinggegevens "op straat"	1	3	3
Mensen	Opzettelijke foutieve handelingen	1	3	3
Programmatuu	Toegangsbeveiliging faalt	1	3	3
Diensten	Uitval elektriciteit	1	3	3
Mensen	Gegevens niet tijdig vernietigd (bewaarplicht)	3	1	3
Mensen	Onopzettelijke foutieve handelingen	3	1	3
Diensten	Afschermen van gegevens van andere scholen	1	2	2
Mensen	Delen van privacy gevoelige info	1	2	2
Diensten	Faillissement	1	2	2
Diensten	Illegaal downloaden door medewerkers	1	2	2
Organisatie	Integriteitsvraagstukken (ontbreken regels/richtlijnen)	1	2	2

14.18 Beslisboom datalek. Zie Beslisboom meldingsformulier Incidenten en datalekken versie 1 (BK - AVG-Kerobei en privacy)



14.19 Bewaartermijnen van persoonsgegevens

De wet is hierover niet erg duidelijk. De PO-Raad en VO-raad zijn voornemens om voor de po- en vo-sector een selectielijst te ontwikkelen, maar deze wordt pas rond 2023 verwacht. Totdat de archiefwet gepasseerd is of totdat PO- en VO-Raad een geldige selectielijst hebben gemaakt hanteert Kerobei tijdelijk in principe het schema bewaartermijnen van Kennisnet.

Schema bewaartermijnen Kennisnet:

Welke gegevens	Wettelijke basis	Uitleg	
1. Specifieke gevallen	specifieke wet	**Specifieke bewaar- c.q. vernietigingstermijn** terug te vinden in wet en regelgeving. Deze specifieke termijn wordt nagekomen. In de tabel in deze handreiking is een opsomming van specifieke bewaartermijnen te vinden (zie bijlage: lijst met termijnen in onderwijswetten).	
2. Europese subsidie (stimuleringsregeling)	ESF	Tot **10 jaar** na vertrek van de betreffende leerlingen/medewerkers moet informatie bewaard worden.	
3. Financiële en fiscale en bekostigingsbescheiden	Artikel 172 lid 3 Wet PO Artikel 130a lid 3 Wet VO	**7 jaar**	
4. Alle gegevens in de leerling administratie PO / VO	Artikel 9 lid 1 (juncto artikel 6 lid 1) bekostigingsbesluit WPO Artikel 6 bekostigingsbesluit VO	Tot **5 jaar** na uitschrijving betreffende leerling blijft diens informatie bewaard in de leerlingadministratie	
5. Onderwijskundig rapport	Artikel 7a Besluit uitwisseling leer- en begeleidingsgegevens	Tot **5 jaar** na uitschrijving bij de latende school.	
6. Persoonsgegevens betreffende de gezondheid van leerlingen	Artikel 18a lid 6 (juncto lod 13) Wet PO 17a lid 14 Wet VO	**3 jaar** na afloop van: (a.) de beoordeling of een leerling is aangewezen op het leerwegondersteunend onderwijs of van het toelaatbaar verklaren van leerlingen tot het praktijkonderwijs of het voortgezet speciaal onderwijs (b.) de advisering over de ondersteuningsbehoefte van de leerling aan het bevoegd gezag van de school, (c.) de toewijzing van ondersteuningsmiddelen of voorzieningen aan de school.	
7. Digitaal leermateriaal	Persoonsgegevens: niet langer bewaren dan noodzakelijk	Po Onderbouw vo	Gegevens huidige schooljaar, plus gegevens voorgaande schooljaar bewaren
		Bovenbouw vo	Gegevens huidige schooljaar, plus de twee voorgaande schooljaren bewaren
8. Alle andere gevallen	Gegevens tot personen herleidbaar	Vernietigen **2 jaar** na uitschrijven of beëindigen relatie	
	Toestemming om na uitschrijven gegevens te bewaren met specifiek doel	Bewaren toegestaan op basis van toestemming (bijv. alumni)	
	Niet tot persoon herleidbaar	Vrij te kiezen	

Toelichting schema:

Dit is een tijdelijke handreiking voor PO-scholen (dec 2020)

Op dit moment hebben nog niet alle ict-systemen en software die scholen gebruiken, de mogelijkheid om gesystematiseerd gegevens te vernietigen of archiveren. Met de leveranciers moet besproken worden om dit in te bouwen of wat de alternatieven zijn om aan de wettelijke bewaar- en vernietigingstermijnen te voldoen.

De betreffende bewaar- en/of vernietigingstermijn gaat pas lopen nadat de leerling de school verlaten heeft (uitgeschreven is). Indien er meerdere bewaartermijnen van toepassing zijn, dan wordt de langste termijn aangehouden.

Het is niet nodig om een back-up (volledig) te wissen om aan bewaartermijnen te voldoen, als aan een aantal specifieke voorwaarden is voldaan.

Is er geen wetgeving waarin iets is vastgelegd over de bewaartermijn? Dan schrijft de AVG voor dat men zelf de bewaartermijnen moet vaststellen. Is het doel waarmee de persoonsgegevens

bewaard worden niet langer van toepassing? Dan moeten de persoonsgegevens vernietigd worden. Bij twijfel anonimiseren en/of verplaatsen naar een beveiligde map.

Vanaf schooljaar 2021-2022 zal Kerobei gegevens van leerlingen en medewerkers verwijderen volgens de richtlijn van Kennisnet. Het betreft in ieder geval het HR-systeem, LVS, Basispoort en Workspace.
Zie:
https://aanpakibp.kennisnet.nl/bewaartermijnen/

Indien de regels bekend zijn zal Kerobei die volgen en opnemen in dit document.

14.20 Model verwerkersovereenkomst versie 4.0

Dit model is te vinden op: https://www.privacyconvenant.nl/het-convenant/
Voor verdere toelichting en voorlichting t.a.v. het gebruik, verwijzen we naar de site van het privacyconvenant.
Sinds 1-8-23 gebruiken we voor beoordeling, ondertekening en opslag van nieuwe verwerkersovereenkomsten de site van dv.kennisnet.nl.

14.21 Convenant digitale onderwijsleermiddelen

Dit model is te vinden op Internet

14.22 Gegevens Functionaris Gegevensbescherming (FG).

stuur een mail naar fg@privacyopschool.nl

14. Lijst met afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
EU	Europese Unie
FG	Functionaris Gegevensbescherming
HRM	Human Resource Management
IBP	Informatie Beveiliging en Privacy
ICT	Informatie Communicatie Technologie
P&O	Personeel en Organisatie
SLA	Service Level Agreement. Hierin staan afspraken tussen aanbieder en afnemer van een dienst of product.
WBP	Wet Bescherming Persoonsgegevens (is op 25-05-2018 vervangen door de AVG).

16. Lijst met begrippen (in de context van het IBP-plan)

Anonimiseren

Anonimiseren is een methode waarbij persoonsgegevens worden bewerkt zodat ze niet meer gebruikt kunnen worden om iemand mee te identificeren. Anonimiseren is onomkeerbaar. De gegevens kunnen dus nooit meer worden teruggeleid tot een persoon. Geanonimiseerde gegevens vallen niet onder de AVG.

Archiefwet

De Archiefwet is een Nederlandse wet die het beheer en de toegang van overheidsarchieven regelt.

Authenticatie

Authenticatie is het bewijzen dat je bent wie je zegt te zijn. Bijvoorbeeld door naar wachtwoord en/of een ander (biometrisch) bewijsmiddel te vragen bij het inloggen op een applicatie. Bij de authenticatie wordt gecontroleerd of het opgegeven bewijs (zoals een wachtwoord) klopt.

Autorisatiematrix

Een schema waarin vast is gelegd wie toegang krijgt tot welke persoonsgegevens. Dat kan op basis van rollen, functies of een mix daarvan.

Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de wettelijke regels voor de bescherming van persoonsgegevens. https://www.autoriteitpersoonsgegevens.nl

Beveiligingsincident

Een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.

Betrokkenen

De personen van wie persoonsgegevens worden verwerkt of gelekt.

Bewaartermijnen

De (wettelijke) periode dat een (persoons)gegeven bewaard moet worden.

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens die betrekking hebben op gevoelige informatie, gedragsproblemen, politieke voorkeur, godsdienst, seksuele voorkeur, gezondheid of een problematische thuissituatie. Bijzondere persoonsgegevens mogen niet worden bewaard of op een andere manier worden gebruikt, tenzij de wet daar toestemming voor geeft.

BIV-classificatie

Het indelen van (persoons)gegevens op basis van beschikbaarheid, integriteit en vertrouwelijkheid zijn.

Bring Your Own Device (BYOD)

BYOD is het gebruiken van je eigen apparatuur voor het uitvoeren van werktaken.

Cloud

De cloud (Nederlands: wolk) staat voor een netwerk dat met alle computers die erop aangesloten zijn, een soort “wolk van computers” vormt. Als je op je werkstation bezig bent, weet meestal niet op hoeveel of op welke computer(s) de software draait of waar die computers precies staan.

Data-integriteit

Data-integriteit heeft betrekking op de juistheid van de informatie. Is het niet verouderd of incorrect?

Datalek

Bij een datalek raken persoonsgegevens verloren of worden ze opgeslagen, aangepast, verzonden of op

een andere manier verwerkt door iemand die daar geen recht toe heeft. Een datalek is een beveiligingsincident.

Dataminimalisatie

Dataminimalisatie betekent niet meer persoonsgegevens verwerken dan nodig. Gebruik alleen persoonsgegevens die je nodig hebt om je doel te bereiken. Je moet je doel niet met minder persoonsgegevens kunnen bereiken en data niet langer bewaren dan noodzakelijk is. Met andere woorden: kan het minder, dan moet het ook met minder.

Dataportabiliteit

Dataportabiliteit betekent dat data overdraagbaar is aan een andere verwerkingsverantwoordelijke in een gestructureerde, gangbare en machineleesbare vorm.

Dataregister

Het dataregister is een register van verwerkingsactiviteiten speciaal voor het onderwijs. Het dataregister is voor een gedeelte al ingevuld en van suggesties voorzien.

DDoS

DDoS staat voor 'Distibuted-denial-of-service'. Pogingen om een computer of netwerk moeilijk bereikbaar te maken door met veel computers tegelijk verzoeken daarop af te vuren.

Derde

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Derde landen

Alle landen buiten de Europese Economische Ruimte: alle EU-landen en Noorwegen, Liechtenstein, IJsland. Derde landen houden zich niet aan de EU-regelgeving als het gaat om privacy.

Documentatieplicht

De documentatieplicht houdt in dat je vast moet leggen op welke manier je je aan de regels van de AVG houdt.

Doelbinding

Je mag persoonsgegevens alleen gebruiken voor een vooraf vastgelegd doel. Als dat doel niet langer bestaat, moet je de persoonsgegevens vernietigen.

DPIA

DPIA is Data Protection Impact Assessment. In het Nederlands heet het gegevensbeschermings-effectbeoordeling. Met een DPIA onderzoek je wat het effect op de privacy van de betrokkenen is bij het verwerken van persoonsgegevens.

ECK-id

Een uniek identificerend nummer (het ECK iD) voor leerlingen en leraren dat scholen kunnen aanmaken via nummervoorziening, een publieke dienst van Kennisnet.

Encryptie

Encryptie is het versleutelen van persoonsgegevens. Door de versleuteling kan een derde partij de gegevens niet inzien. Alleen de juiste zender en ontvanger beschikken over de sleutel.

Functionaris voor Gegevensbescherming

Iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG).

Gezamenlijke verwerkingsverantwoordelijke
Twee of meer verwerkingsverantwoordelijken die gezamenlijk verantwoordelijk zijn voor de verwerking van persoonsgegevens. Bijvoorbeeld een integraal kindcentrum.
Governance
Besturen, zeggenschap hebben en toezicht houden.
Grondslag
De (wettelijke) basis waarop je persoonsgegevens verwerkt. Er zijn 6 mogelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
Hacker
Een hacker is iemand die op zoek gaat naar zwakke plekken in computers, software of computernetwerken en vervolgens inbreekt.
Informatieplicht
Het aan betrokkenen bekendmaken van wat je met hun persoonsgegevens je doet.
Informatievoorziening
het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
Inzage
De mogelijkheid die betrokkenen hebben om hun eigen persoonsgegevens in te zien of een overzicht te krijgen van de persoonsgegevens die worden verwerkt.
ISO
Internationale organisatie voor standaardisatie. Een ISO norm voor informatiebeveiliging is de ISO 27001 of 27002 of 9001.
Keten
De samenwerking in de onderwijsketen: van brancheorganisatie van educatieve uitgevers en softwareleveranciers tot koepelorganisaties van scholen.
Kwetsbaarheid
Een fout in de toegangsbeveiliging waardoor onbevoegden toegang krijgen tot software en systemen en mogelijk ongewenste handelingen kunnen uitvoeren. Een kwetsbaarheid kan leiden tot een datalek.
Leveranciers
Aanbieders van ict- of leermiddelen.
Manager IBP
Hiermee wordt de Bovenschoolse ICT'er bedoeld (BIC), voorheen stafmedewerker ICT.
Meldplicht datalekken
De plicht tot het doen van een melding doen bij de Autoriteit Persoonsgegevens (AP) zodra er een ernstig datalek geconstateerd is.
OKR
Het onderwijskundig rapport.
Ontvanger
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan aan waaraan persoonsgegevens worden verstrekt.
Opt-in
De mogelijkheid om ervoor te kiezen je persoonsgegevens te delen.

Opt-out
De mogelijkheid om ervoor te kiezen je persoonsgegevens niet te delen.
Ouders
Waar ouders staat worden de wettelijke vertegenwoordigers bedoeld: personen die de ouderlijke verantwoordelijkheid dragen voor het kind. Dit kunnen ook verzorgenden zijn.
Persoonsgegevens
Alle gegevens waarmee direct of indirect een natuurlijk persoon (mens) kan worden geïdentificeerd. Het kan bijvoorbeeld gaan om een naam, BSN-nummer, geboortedatum, telefoonnummer of IP-adres.
Privacy
Het recht om met rust te worden gelaten, om te weten en te bepalen wat er met gegevens over jou gebeurt en om te weten wie de beschikking heeft over jouw persoonsgegevens.
Privacy by default
Standaard producten of diensten staan zo ingesteld dat privacy wordt gewaarborgd. Alle opties om persoonsgegevens te delen staan standaard “uit”.
Privacy by design
Bij het ontwerpen van producten en diensten, zoals software ervoor zorgen dat persoonsgegevens standaard goed beschermd worden.
Privacy Officer
Kerobei heeft geen privacy officer, deze rol wordt vervuld door de manager IBP.
In het vo meestal betrokken bij de uitvoering van IBP. Deze rol kan ook afhankelijk van het soort onderwijs (po of vo) en van de grootte van de organisatie, ook vervuld worden door een manager IBP, verantwoordelijke IBP, informatiemanager, Security Officer, functioneel beheerder, ict-beheerder, ict-coördinator of kwaliteitsmedewerker.
Privacybijsluiter
Bijlage bij de verwerkersovereenkomst met een leverancier van ict-diensten. In de privacybijsluiter wordt beschreven wat de dienst doet, wie daarvoor verantwoordelijk is, welke persoonsgegevens er betrokken zijn, waar de gegevens worden opgeslagen.
Privacyconvenant
Het stelsel van afspraken die scholen en aanbieders van digitale diensten met elkaar maken, waarbij iedereen de afspraken op dezelfde manier uitlegt.
Profilering
Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.
Pseudonimiseren
Een methode waarbij identificerende persoonsgegevens met een bepaald algoritme worden vervangen door versleutelde gegevens (het pseudoniem). Het algoritme kan aan een persoon steeds hetzelfde pseudoniem toekennen, waardoor informatie uit verschillende bronnen kan worden gecombineerd. Na de encryptie is het dus nog steeds mogelijk om de betrokkene te identificeren: met behulp van het algoritme kan de versleuteling namelijk weer worden teruggedraaid. Een pseudoniem is dus een persoonsgegeven.
Register van verwerkingsactiviteiten
Een register met informatie over verwerkingen van persoonsgegevens.

Risicoanalyse
Het analyseren van de kans dat een dreiging werkelijkheid wordt en de gevolgen hiervan.
Samenwerkingsverband
De organisatie die in het kader van het passend onderwijs gaat over de toewijzing van extra hulp en ondersteuning voor leerlingen. Alle scholen in de regio van het samenwerkingsverband zijn hierbij aangesloten.
Schoolbestuur
Het schoolbestuur is het bevoegd gezag en daarmee eindverantwoordelijk voor alles dat met IBP te maken heeft.
SLA
Service Level Agreement – het onderhoudscontract tussen school en een leverancier van systemen, software of diensten.
Subverwerker
De leverancier van de leverancier van de school. Degene die in opdracht van de verwerker verwerkingen doet. De verwerker is ervoor verantwoordelijk dat de subverwerker op de hoogte is van afspraken met de verwerkingsverantwoordelijke.
Transparantie
Helder zijn over de persoonsgegevens die je verzamelt en wat je er mee doet.
Veilige landen
Alle EU-landen en Noorwegen, Liechtenstein, IJsland (samen de EER) die zich houden aan de EU-regelgeving als het gaat om privacy.
Vernietigen
Het definitief verwijderen van gegevens, zodat de persoonsgegevens niet meer aanwezig of terug te halen zijn.
Vertegenwoordiger
Een in de EU gevestigde natuurlijke persoon of rechtspersoon die door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen.
Verwerken
Alles wat er met persoonsgegevens wordt gedaan, wordt in de wet verwerken genoemd. Verwerken is dus onder meer: online en offline persoonsgegevens verzamelen, kopiëren, opslaan, verspreiden, publiceren, delen én uitwisselen. Het maakt dus niet uit wat je doet met persoonsgegevens: alles noemen we verwerken en valt onder de wettelijke bescherming.
Verwerker
Degene of de organisatie die handelt in opdracht van de verwerkingsverantwoordelijke, zoals de leverancier van het leerling administratiesysteem. Deze mag alleen verwerkingen doen waarvoor hij uitdrukkelijk opdracht krijgt.
Verwerkingsverantwoordelijke
Degene die het doel en de middelen bepaalt bij het verwerken van persoonsgegevens, zoals een schoolbestuur.
Workspace Door Kerobei gebruikte netwerkoplossing van Google, voorheen G-Suite genoemd.