ontwikkelen
in ontmoeting

KEROBEI

InformatieBeveiligings- en Privacybeleid (IBP)

Kerobei

Inhoudsopgave

Versie	Status	Datum	Auteur	Omschrijving
1.0	concept	10-03-2017	Ton Pouls	Eerste concept ter bespreking in verbeterteam ICT
1.1	concept	16-09-2017	Ton Pouls	Tweede concept ter bespreking in verbeterteam ICT
1.3	concept	06-12-2017	Ton Pouls	Derde concept ter bespreking in verbeterteam ICT en ter beschikkingstelling aan GMR
1.4	concept	17-01-2018	Ton Pouls	Vierde concept ter beschikkingstelling aan WPDO
2.0	concept	09-04-2018	Ton Pouls	Vijfde concept ter beschikkingstelling aan GMR

Vastgesteld door CvB Kerobei

Versie	Datum	Naam	Functie
2.0	26-04-2018	**Hans Soentjens**	**Voorzitter CvB Kerobei**

Instemming gedragscode

Versie	Datum	Naam
2.0	25-04-2018	**GMR**

1 Inleiding.

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 vanaf 25 mei 2018 nog maar één privacywet geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (WBP) geldt dan niet meer. De AVG is een verordening die rechtstreeks verplichtingen oplegt aan degene(n) die persoonsgegevens verwerken en rechten toekent aan betrokkenen. Ook Nederlandse scholen moeten in 2018 voldoen aan de nieuwe wetgeving.
Als de Algemene Verordening Gegevensbescherming (AVG) van toepassing is, hebben organisaties die persoonsgegevens verwerken meer verplichtingen. Er wordt in de AVG meer nadruk gelegd op de verantwoordelijkheid van organisaties (scholen) zelf. Scholen moeten niet alleen de **wet naleven**, zij moeten kunnen **aantonen** dat zij zich aan de wet houden.

1.2 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.
- Veerkracht: de mate waarin we omgaan met storingen en in staat zijn de systemen in oude staat te herstellen.

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.

1.3 Toelichting privacy.

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Onder persoonsgegevens wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. De wet noemt als voorbeelden van verwerking: *het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.*

1.4 Vervlechting informatiebeveiliging en privacy.

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen Kerobei.

2 Doelen en reikwijdte.

2.1 Doelen.

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.

Dit beleid is 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.

2.2 Reikwijdte.

- Het informatiebeveiligings- en het privacy beleid binnen Kerobei geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de

verantwoordelijkheid van Kerobei. Het beleid heeft betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites.

- Het 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 andere betrokkenen waarvan Kerobei persoonsgegevens verwerkt.
- In het beleid ligt de nadruk op 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 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 binnen Kerobei heeft 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
  - Beleid inzake aanschaf en gebruik van digitale leermiddelen

3 Uitgangspunten.

3.1 Algemene beleidsuitgangspunten.

De belangrijkste beleidsuitgangspunten bij Kerobei zijn:

- Informatiebeveiliging en privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking treedt en de WBP dan vervangt).
  De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen, waarbij 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 zijn persoonsgegevens van belang is.
- 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 geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten.
- De school 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

moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.

- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij Kerobei geclassificeerd (zie hfst **6.2**). De classificatie is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik gemaakt wordt van de classificatie. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- Kerobei sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant *Digitale onderwijsmiddelen en privacy* (zie bijlage **14.19**) en de bijbehorende model verwerkersovereenkomst, zie bijlage **14.18**. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis. Alle verwerkersovereenkomsten die Kerobei heeft afgesloten zijn voor alle medewerkers in te zien en worden toegelicht in het document *Verwerkersovereenkomsten Kerobei* (Boekenkast M-schijf).
- Er wordt van alle medewerkers, leerlingen, ouders, (geregistreerde) bezoekers en externe relaties verwacht 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 **14.8**
- Informatiebeveiliging en privacy is bij Kerobei een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij Kerobei vanaf de start rekening gehouden met informatiebeveiliging en privacy.

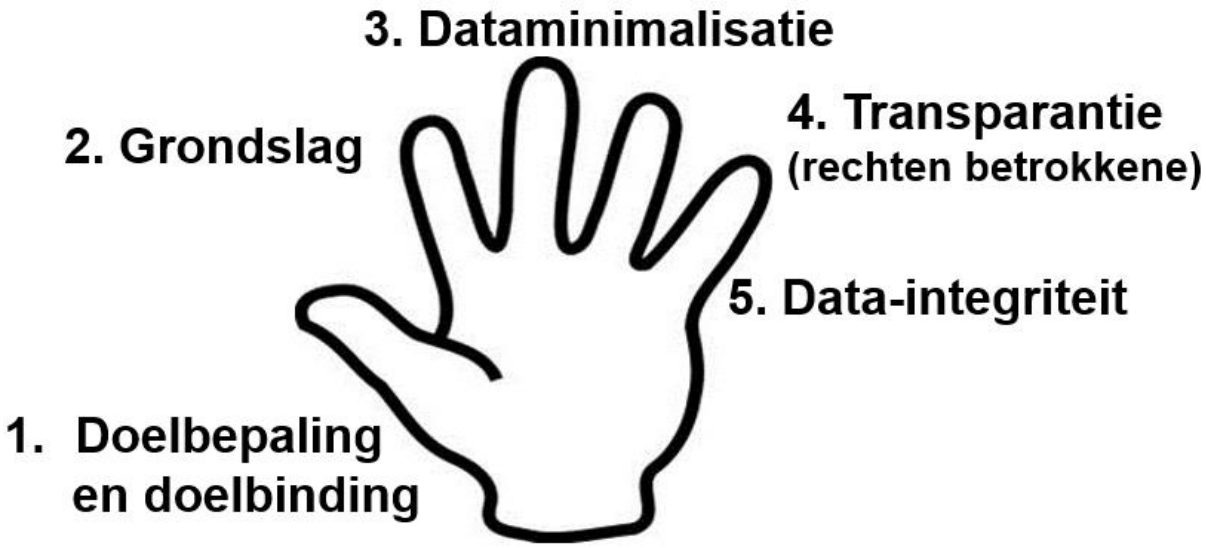
3.2 Uitgangspunten privacy.

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij Kerobei zijn:

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 **14.17**
4. **Transparantie**: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.



4 Wet- en regelgeving.

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

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

Hiernaast zijn de bepalingen van het convenant *Digitale onderwijsmiddelen en privacy* (zie bijlage **14.19**) leidend bij het maken van afspraken met leveranciers.

5 Organisatie.

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.

5.1 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.

5.1.1 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 stafmedewerker ICT. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen. Kerobei heeft Dhr. Theo Kusters aangesteld als FG. Zie bijlage **14.20**

5.1.2 Stafmedewerker ICT (manager IPB).

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

5.1.3 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 hierbij een voorbeeldrol ten opzichte van hun medewerkers.

5.2 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 stafmedewerker ICT neemt hiertoe het initiatief.

5.3 Sturend (tactisch).

De stafmedewerker ICT is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op uitvoerend niveau. De Stafmedewerker ICT 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

5.4 Uitvoerend (operationeel).

5.4.1 Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelshandboek, waarin ook verwijzingen naar dit document zijn opgenomen (is nog niet geregeld, afgesproken op 180129; het personeelshandboek dient per 1-8-2018 gereed te zijn). 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)

5.4.2 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 Stafmedewerker ICT.
Zie bijlage **14.1** voor een schematische weergave.

6 Controle en rapportage.

Dit informatiebeveiligings- en privacybeleid wordt minimaal jaarlijks getoetst en bijgesteld. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

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.

6.1 Voorlichting en bewustzijn.

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij Kerobei het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de leidinggevenden (zie hfst **5.4.2**) met het College van Bestuur als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse.

Bij Kerobei heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses, zie bijlage **14.15.** Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang voor de informatievoorziening.

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 **14.15**.)

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 backup/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 telewerken/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 bewerken wordt een verwerkersovereenkomst afgesloten.

6.3 Incidenten en datalekken.

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 **14.16**

6.4 Controle, naleving en sancties.

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

van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het CvB vast te stellen reglement.
Mocht de naleving ernstig tekortschieten, dan kan Kerobei de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

7 Privacyreglement Kerobei.

De huidige versie van het privacyreglement is opgenomen in bijlage **14.2**

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 is een model reglement opgenomen dat door de scholen van Kerobei gebruikt kan worden.

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 toetsgegevens, 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.
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 **14.9.**
In bijlage **14.12** 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 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 wettelijke grondslag 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 en andere personen, ter beoordeling van de directeur, die persoonsgebonden informatie verwerken wordt gevraagd de

gedragscode van Kerobei te ondertekenen. Zie bijlage **14.8** Hiervoor is toestemming verleend door de GMR op 25-04-2018.

10 Datalekken en melding hiervan.

10.1 Inleiding.

Sinds 1 januari 2016 is de meldplicht datalekken van kracht. De meldplicht vormt een toevoeging aan de Wet Bescherming Persoonsgegevens (WBP): zowel bedrijven als overheden moeten voortaan direct melding doen als er een datalek heeft plaatsgevonden, bijvoorbeeld in geval van een hack of diefstal van een USB-stick met belangrijke informatie.

Kerobei vindt het van groot belang, niet alleen om aan de Wet op Bescherming Persoonsgegevens en na 25 mei 2018 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 **14.17**
- 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 hebbende 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 z.s.m. wordt gemeld (zie bijlage **14.16Fout! V erwijzingsbron niet gevonden.**) 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 14.10
Model responsible disclosure voor leerlingen, zie bijlage 14.11

10.3 Wat is een datalek?

Een datalek is een inbreuk in verband met persoonsgegevens. Denk aan het verkrijgen van toegang tot, vernietiging, wijziging of vrijkomen van persoonsgegevens (van leerlingen, ouders of medewerkers) bij Kerobei als organisatie, zonder toestemming van Kerobei. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. Zie bijlage **14.16** (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 72 uur!). Mocht het datalek ongunstige gevolgen hebben voor de levenssfeer van betrokkenen, dan dient men naast de Autoriteit Persoonsgegevens ook de betrokkenen in te lichten. De maximale boete voor het niet op tijd melden is in de nieuwe wet maar liefst 810.000 euro of maximaal 10% van de omzet.
Alle meldingen worden bijgehouden in een incidentenregister. Dit is een separaat document.

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 **14.16** en de gedragscode, bijlage **14.8**):

- 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 voorgenoemde tekst besproken, neem dan eerst contact op met de directeur van de school. Deze neemt vervolgens contact op, telefonisch of per mail, met het College van Bestuur van Kerobei, Huub Hovens, 077-396 8888, privacymelding@kerobei.nl I.o. zal bekeken worden hoe de procedure vervolgd wordt.
Bij vermeende datalekken op het stafbureau dient meteen contact te worden opgenomen met het CvB.

(zie de beslisboom datalekken, bijlage 14.16)

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 leerlinggegevens. 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 leerlinggegevens, 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.
Zie schema in bijlage 14.13

11.2 Welke gegevens bewaren de 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 **14.12**
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 **14.14**

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 **14.7**

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, schoolgids... dat ze hun goedkeuring te allen tijde kunnen intrekken. Vanzelfsprekend is toestemming in vrijheid gegeven en geldt ondubbelzinnig voor een vooraf gesteld doel.

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 is te vinden in bijlage 14.5. Toelichting toestemmingsformulier, zie bijlage 14.6

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 14.15 risico-classificatie).

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)
- Stafmedewerker ICT (ST)
- 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 8 karakters, 1 hoofdletter, 1 kleine letter, 1 cijfer en 1 symbool. 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!).

Aanbevolen:
-Gebruik een zin: Ckjwi5rwhtki! = Computers kunnen je wachtwoord in 5 seconden raden wanneer het te kort is!
-Een wachtwoord wordt niet gedeeld.
-Een wachtwoord wordt min. een keer per jaar veranderd.
-Een wachtwoord wordt niet hergebruikt.
-Gebruik voor elk programma een eigen wachtwoord.
-Gebruik, indien mogelijk, in de onderbouw een combinatie van afbeeldingen.

13.1.1 Bewaren van wachtwoorden.

Kerobei is op zoek naar een wachtwoordkluis. Zo lang 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, 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 moet worden gedocumenteerd.
Kerobei is bezig met het maken van beleid.
Dit zal voor 25 mei 2018 toegevoegd worden.

13.3 Documentatieplicht.

Kerobei houdt een register van alle verwerkingsactiviteiten bij. Hiervoor wordt verwezen naar M:\Kerobei\Boekenkast\Kerobei Vastgesteld beleid\Organisatie\...Dataregister
Kerobei is bezig met het maken van beleid, Dit zal voor 25 mei 2018 toegevoegd 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 verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen

Sturend (tactisch)	Stafmedewerker ICT (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) Stafmedewerker ICT	• 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/ Proceseigenaren waaronder: ict, personeel (HRM / P&O), Facilitair, onderwijs, financiën, inkoop en administratie	• **Classificatie / risicoanalyse** *in samenwerking met stafmedewerker ICT (verantwoordelijke IBP)* • Toegangsbeleid zowel fysiek als digitaal vaststellen en 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	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

	Stafmedewerker ICT	netwerkdiensten waarvoor zij specifiek bevoegd zijn. • *Samen met functioneel beheer en ICT* beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	

Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen** **Vanuit de Wiki**
Uitvoerend (operationeel)	Stafmedewerker ICT Functioneel beheerder: Unilogic 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. • 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.	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

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 *Doelen*	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. 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. b. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op Kerobei rust. c. 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.

d. 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.

e. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen (levensbelang).

f. 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 technische 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	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.
Beperken verwerking	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.
Kennisgevingsplicht	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 Modelreglement Internet en sociale media.

Het modelreglement 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.

De geel gearceerde velden in de afspraken kunnen door de scholen afzonderlijk worden aangepast.

Modelreglement Internet en sociale media voor Kerobei.

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, en 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 leraar 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 [wel/niet] toegestaan. Een leraar 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 kantine, 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 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 is 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'.

    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 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.]

11. [Het leggen van contact, het volgen van elkaar of 'vriend worden', is een bewuste keuze waar goed over nagedacht is. We weten wie de andere persoon is.]
    en/of:
    [Leerlingen en medewerkers van SCHOOL worden niet met elkaar 'vriend' op sociale media, tenzij het gaat om een door de medewerkers gebruikt professioneel account (waar geen persoonlijke informatie over de medewerker is geplaatst).]

12. 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, [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 de stage- juf 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 sociale media.

Logo school	**Formulier toestemming gebruik beeldmateriaal en sociale media Schoolnaam**	

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 het ouderportaal	☐ Informeren van ouders en leerlingen over de onderwijsactiviteiten zoals schoolreisjes, excursies, schoolfeesten, etc. Ouders en leerlingen informeren over activiteiten en ontwikkelingen op en om school
In de (digitale) nieuwsbrief	☐ Ouders en leerlingen informeren over activiteiten en ontwikkelingen op en om 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.

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.

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.

Hierbij verklaart ondergetekende dat alle in dit formulier aangevinkte items van toepassing zijn.	
Datum	
Naam ouder/verzorger	
Naam kind	
Groep	
Handtekening ouder/verzorger	

14.6 Toelichting 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 (Voor)aanmeldingsformulier Kerobei.

Logo school	**VOORAANMELDINGSFORMULIER BASISSCHOOL SCHOOLNAAM**	

GEGEVENS LEERLING

* Doorhalen wat **niet** van toepassing is

Achternaam			
Voorvoegsel			
Voornamen			
Roepnaam			
Geslacht (M/V)			
Adres			
Postcode/woonplaats			
Telefoon thuis		Geheim: Ja/Nee*	
Geboortedatum			
Geboorteplaats		Geboorteland	
Nationaliteit 1		Gezindte	
Nationaliteit 2		Datum in Nederland	
Huisarts en praktijk		BSN	
Welke thuistaal, behalve Nederlands, spreekt u met uw kind?			
Gezinssamenstelling: (namen broers en zussen met leeftijd)			

Medische gegevens	
Allergisch voor	
Medicijnen	
Algemene medische gegevens	

Voorschoolse educatie			
Naam peuterspeelzaal /kinderdagverblijf		Vanaf	
VVE indicatie	Ja/Nee*		
Zij-instromer van school		Groep	
Zorgtraject	Ja/Nee*		
Welk *(bijv. extra gesprekken op psz omtrent ontwikkeling, inzet audiologisch centrum, integrale vroeghulp, medische trajecten, bureau jeugdzorg, BCO, enz.)*			

Ik ga ermee akkoord dat de school bij andere instellingen relevante informatie over de ontwikkeling van het kind opvraagt.	Ja/Nee*

GEGEVENS VERZORGERS			
Gegevens eerste verzorger: wettelijke / biologische vader / moeder / voogd *			
Achternaam		Voorvoegsel	
Roepnaam		Geboortedatum	
Geboorteland		Nationaliteit	

Beroep			
Mobiele telefoon		Geheim	Ja/Nee*
E-mailadres			
Gezinssamenstelling	Alleenstaand – Gehuwd – Samenwonend - Geregistreerd Partnerschap – Gescheiden *		
Gegevens tweede verzorger: wettelijke / biologische vader / moeder / voogd *			
Achternaam		Voorvoegsel	
Roepnaam		Geboortedatum	
Geboorteland		Nationaliteit	
Beroep			
Mobiele telefoon		Geheim	Ja/Nee*
E-mailadres			
Gezinssamenstelling	Alleenstaand – Gehuwd – Samenwonend - Geregistreerd Partnerschap – Gescheiden *		
Indien ander adres dan leerling			
Adres		Postcode	
Woonplaats		Eenoudergezin	Ja/Nee*
Extra telefoonnummer met naam			

GEZINSSITUATIE	
De gezinssituatie is als volgt geregeld	☐ Het gezag berust bij beide ouders gezamenlijk
	☐ Alleen moeder / 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

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 het ouderportaal	☐ Informeren van ouders en leerlingen over de onderwijsactiviteiten zoals schoolreisjes, excursies, schoolfeesten, etc. Ouders en leerlingen informeren over activiteiten en ontwikkelingen op en om school
In de (digitale) nieuwsbrief	☐ Ouders en leerlingen informeren over activiteiten en ontwikkelingen op en om 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.

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.

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.

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 vóórdat 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 gaat ermee akkoord dat de gegevens kunnen worden gecontroleerd.
Bij het verwerken van deze gegevens houden wij ons aan de Algemene Verordening Gegevensbescherming (AVG).

Eerste verzorger		Tweede verzorger	
Datum		Datum	
Handtekening		Handtekening	

14.8 Gedragscode ICT-gebruik en privacy medewerkers Kerobei.

Gedragscode privacy Kerobei.

Van de medewerkers binnen Kerobei wordt verwacht dat zij:

- op een professionele manier communiceren en handelen conform het Informatie beveiligings- en privacy beleid.
- persoonsgegevens die door Kerobei verzameld zijn, alleen gebruiken voor het doel waarvoor ze verzameld zijn. Indien deze gegevens ook nodig zijn voor andere doeleinden en er is geen andere rechtsgrond van toepassing, dan wordt hiervoor expliciete toestemming gevraagd (en vastgelegd).

Bijvoorbeeld: Naam, achternaam, geboortedatum en (e-mail)adres van kinderen of hun ouders/verzorgers die in het kader van inschrijving zijn doorgegeven aan de school, mogen niet zonder toestemming door een school doorgegeven worden aan derden, zoals uitgevers voor het gebruik van digitaal leermateriaal of andere doeleinden, tenzij met deze derden een verwerkersovereenkomst afgesloten is.

- gegevens alleen verstrekken aan de personen of organisaties die hiertoe gerechtigd zijn.
- gegevens alleen opslaan op de daarvoor ingerichte en aangewezen ICT-systemen en/ of fysieke bewaarplaatsen.
- wachtwoorden die zijn verstrekt door Kerobei voor de (fysieke dan wel digitale) toegang van gegevens zorgvuldig bewaren en niet overhandigen aan derden. Tevens dient voorkomen te worden dat wachtwoorden kunnen worden afgekeken bij het intypen.
- bij het verlaten van de werkplek dient het device waarop gewerkt wordt vergrendeld te worden.
- geen niet werk gerelateerde contacten met leerlingen onderhouden via het schoolaccount, sociale netwerken of anderzijds via Internet.
- Geen persoonsgegevens versturen op een niet beveiligde verbinding.
- geen formulieren en/of documenten met persoonsgegevens op hun bureau laten liggen.
- documenten met persoonsgegevens printen via een mailbox zodat ze niet bij de printer blijven liggen.
- Voorzichtig zijn met het gebruiken van openbare wifi netwerken voor het verwerken van persoonsgegevens van leerlingen.
- geen dossiers met persoonsgegevens in niet afgesloten kasten bewaren.
- gebeurtenissen en/of misstanden die te maken hebben met de verwerking of toegang tot informatie melden aan de directeur van de school. *(De directeur bepaalt of de meldingsplicht van toepassing is bij een incident en zet deze in gang indien van toepassing, zie bijlage :Beslisboom* hfst 14.16
  Hierbij valt te denken aan:
  -verloren USB-stick.
  -foutief geadresseerde e-mails.
  -het kunnen inzien van privacygevoelige gegevens die niet voor hem/haar bestemd zijn. -alle andere situaties waarin persoonsgegevens bij onbevoegden zijn terechtgekomen

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, 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
(M:\Kerobei\Boekenkast\Kerobei Personeelinformatie\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:

14.9 Informatiebeveiligingsbeleid Kerobei.

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. Unilogic beheert ons netwerk en onze data op professionele wijze en wij vertrouwen als stichting op de expertise en beveiliging van dit bedrijf. Unilogic 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 de tool EDUgrip beheer.

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 netwerk van Kerobei via de applicatie 'Verbinding maken via extern bureaublad'. Zij moeten daar met hun persoonlijke inloggegevens inloggen.
Door nieuwsberichten voor alle Kerobei personeel 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.

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 Unilogic, de ICT-beheerder van de school of door de stafmedewerker ICT gedaan worden; het beheer ervan geschiedt 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 Unilogic, de ICT-beheerder van de school of de stafmedewerker ICT.
Bij beëindiging van het dienstverband wordt het account op de eerstvolgende werkdag volgend op de datum van uittreding verwijderd 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. Er is een hyperlink beschikbaar waarmee medewerkers het wachtwoord kunnen wijzigen zonder tussenkomst van anderen.

Medewerkers die hun wachtwoord zijn vergeten kunnen dit via Unilogic 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.
Voor alle overige wijzigingen wordt een autorisatietabel bijgehouden door de stafmedewerker ICT en ter beschikking gesteld aan Unilogic. Alleen de personen in deze tabel mogen bepaalde wijzigingen op school aanvragen. Deze tabel wordt in elk geval jaarlijks en, indien nodig vaker, bijgewerkt.
Van medewerkers wordt verwacht dat zij hub 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. De medewerkers die toegang hebben tot deze gegevens werken middels een eigen, voor hun werkzaamheden afgestemde, account. Alle andere medewerkers hebben alleen toegang in *Mijn Merces,* 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 (boekenkast).

Hardware

Hardware waarmee toegang wordt verkregen tot het netwerk van Kerobei moet worden gecertificeerd en geïnstalleerd door Unilogic. Alleen dan kan een apparaat op het netwerk inloggen. Omdat het netwerk en alle hardware door dezelfde partij op professionele wijze is geconfigureerd en up-to-date wordt gehouden, wordt de kans op hacken aanzienlijk verkleind.
Aangezien al onze data staat opgeslagen in het datacenter van Unilogic 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 Unilogic 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.

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 **14.8.** Hierin staan alle richtlijnen omtrent dit onderwerp.

14.10 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.

14.11 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.

14.12 Welke gegevens verwerkt Kerobei? Voorbeeldteksten voor ouders en derden.

De school bewaart verschillende gegevens over uw kind in een leerling dossier. De school en de ouders mogen deze leerling gegevens inzien. In speciale gevallen mogen derden dat ook.

De basisschool houdt van elke leerling een leerling dossier bij. Daarin bewaart de school:
- Gegevens over inschrijving en uitschrijving.
- Gegevens over afwezigheid.
- Adresgegevens.
- Gegevens die nodig zijn om het leerlinggewicht vast te stellen.

Ook de volgende gegevens mag de school bewaren:

- Gegevens over de ondersteuningsbehoefte, als uw kind die heeft.
- Gegevens over de gezondheid die nodig zijn voor eventuele speciale begeleiding of voorzieningen;
- Gegevens over de vorderingen en de resultaten van uw kind.

De school mag de meeste gegevens nog 2 jaar bewaren nadat uw kind van school is gegaan. De basisschool moet langer bewaren:

- Gegevens over verzuim en in- en uitschrijving (5 jaar nadat de school uw kind heeft uitgeschreven).
- Gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen (3 jaar na vertrek van de leerling).

Adresgegevens van (oud-)leerlingen mag de school bewaren, bijv. voor het organiseren van reünies.

Inzage en correctie leerling gegevens

Als ouder heeft u het recht om de gegevens over uw kind in te zien (inzagerecht). U maakt hiervoor een afspraak met de school. Terwijl u de gegevens inziet, blijft iemand van de school aanwezig. Als ouder heeft u ook correctierecht. U kunt de school verzoeken feitelijke onjuiste gegevens in het leerling dossier van uw kind te verbeteren of te verwijderen.
Heeft u geen ouderlijk gezag meer, bijvoorbeeld na een echtscheiding? Ook dan moet de school u inzage geven in de leerling gegevens over uw kind. Dit staat in het Burgerlijk Wetboek. U moet dan zelf de directie van de school om deze informatie vragen.

Inzage leerlinggegevens door derden

Soms is de school verplicht om gegevens aan bepaalde professionals te geven. Bijvoorbeeld bij:
- de overgang naar een andere school, zoals een andere basisschool, het voortgezet onderwijs (vo) of het speciaal basisonderwijs (sbo).
- inzage door de Inspectie van het Onderwijs (IvhO).
- vermoedens van kindermishandeling.

- noodsituaties.

In andere gevallen moet u als ouder eerst toestemming geven, voordat derden de gegevens van uw kind mogen inzien.

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

Welke gegevens mogen worden uitgewisseld met OSO (Overstapservice Onderwijs)

Jaarlijks stappen ruim 175 duizend leerlingen over van het PO naar het VO. Het is wettelijk bepaald dat hierbij leer- en begeleidingsgegevens moeten worden uitgewisseld. Dit overstapdossier bevat veel gevoelige gegevens over de leerlingen. Ouders hebben het recht om het rapport voor uitwisseling in te zien. In de wet is ook vastgelegd welke leer- en begeleidingsgegevens uitgewisseld mogen worden:

- Gegevens over in- en uitschrijving;
- Gegevens over afwezigheid.
- Adresgegevens.
- Gegevens die nodig zijn om te berekenen hoeveel geld de school krijgt.
- Het onderwijskundig rapport.
- Gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen.
- Gegevens over de vorderingen en de resultaten van de leerling.
  Verslagen van gesprekken met de ouders.
- De resultaten van eventueel psychologisch onderzoek.

(De “oude” school mag dus niet het gehele leerlingdossier ongezien doorsturen, maar alleen die gegevens die nodig zijn om de leerling op de nieuwe school goed te begeleiden en te laten leren.)

Om deze gegevens veilig uit te wisselen is een digitale service ontwikkeld door de PO- en VO-raad, waarmee de gegevens rechtstreeks tussen de administratiesystemen van scholen uitgewisseld kunnen worden. Deze service, de Overstapservice Onderwijs (OSO) genaamd, wordt door veel schoolbesturen gebruikt. In de praktijk gebeurt het echter ook nog vaak dat gegevens op papier worden uitgewisseld. Dit kost de scholen veel extra tijd, omdat de gegevens handmatig ingevoerd dienen te worden in de administratiesystemen. Met OSO kan ook de privacy beter beschermd worden, omdat gewerkt wordt met de laatste beveiligings- en gegevensstandaarden waaraan leveranciers moeten voldoen. De huidige DOD-koppeling die ook nog wel gebruikt wordt, wordt daarom uit gefaseerd. Het gebruik van OSO vraagt echter wel om goede (regionale) afspraken tussen scholen over de gegevens die aangeleverd moeten worden en de momenten waarop dit moet gebeuren. Alle scholen van Kerobei zijn gecertificeerd voor OSO en alle betreffende medewerker zijn bekend met de werkwijze. Voor Kerobei is OSO een standaard. Er wordt nauw samengewerkt met het VO in de regio en uiteraard met de samenwerkingsverbanden.
Meer informatie over OSO: https://www.overstapserviceonderwijs.nl/

14.13 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	Beide ouders. Zij bepalen welke andere personen alle informatie mogen	Indien er signalen zijn van kindermishandeling/huiselijk geweld.	

ouders het gezag hebben.	verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).		
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

14.14 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.
- 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 plaats vond op grond van een gerechtvaardigd belang. De school maakt een afweging van het privacybelang van de leerling, tegenover het belang van de school om gegevens wél te gebruiken.
- De leerling en/of zijn ouders hebben **het recht om bij toestemming**, ook een beperkte toestemming te geven of toestemming te onthouden voor een onderdeel van de verwerking (**granulaire toestemming**).
- De leerling en/of zijn ouders hebben het **recht dat verbeteringen**, aanvullingen of verwijderingen aan alle andere partijen worden doorgegeven aan wie een organisatie de persoonsgegevens van betrokkene heeft verstrekt.
- **Het recht op 'bevriezing van de verwerking'** van zijn gegevens
- De betrokkene heeft het '**recht om te worden vergeten'** door het volledig wissen van de persoonsgegevens, tenzij er een wettelijke bewaarplicht geldt of het verwijderen in strijd is met de vrijheid van meningsuiting. Voor het onderwijs is dit recht minder relevant omdat 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.

14.15 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).

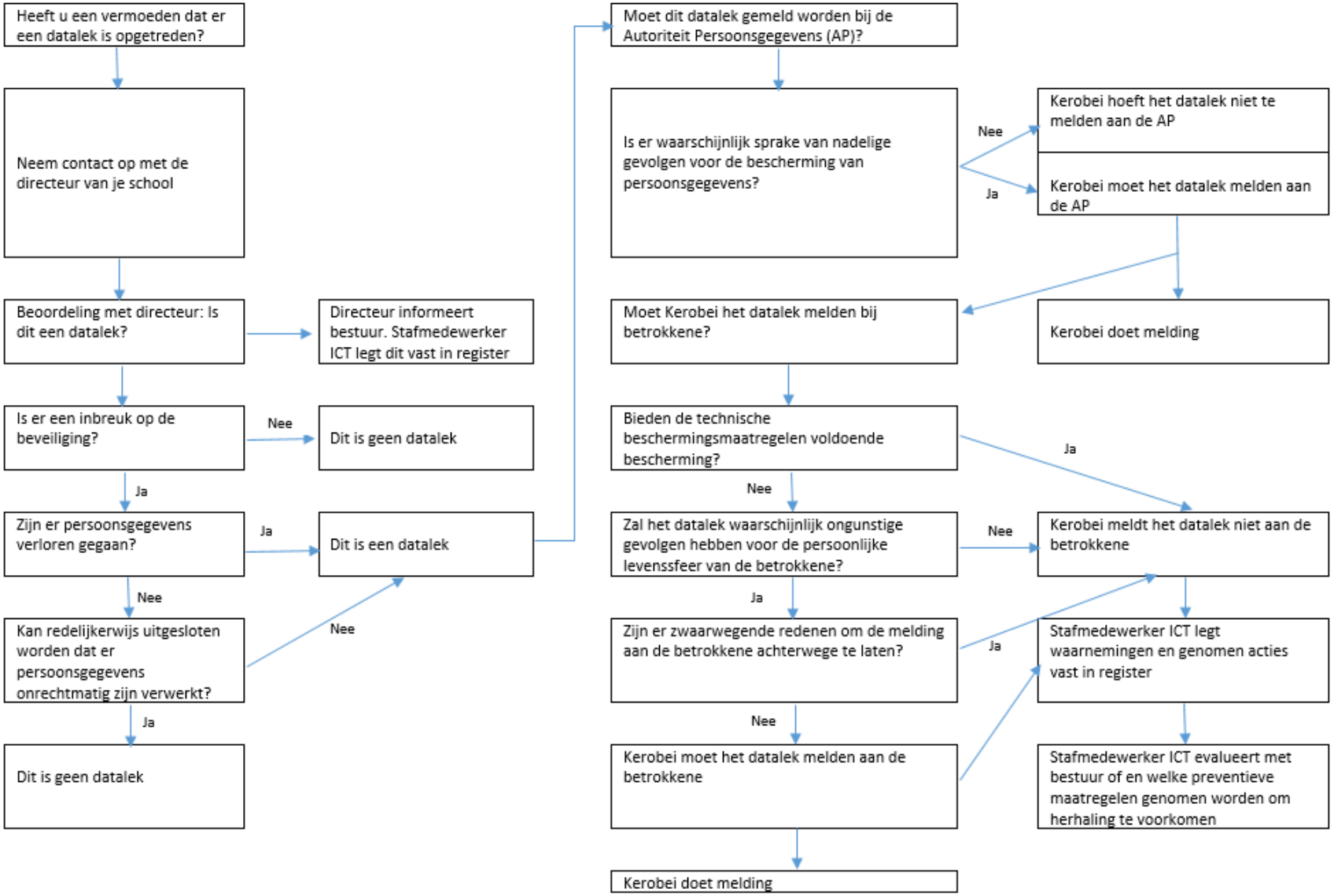
Impact effect als het risico waarheid wordt/nadelige gevolgen:

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
Programmatuur	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

14.16 Beslisboom datalek.



14.17 Bewaartermijnen van persoonsgegevens.

De wet is hierover niet erg duidelijk.
In principe geldt voor leerlinggegevens een standaard bewaartermijn van 2 jaar nadat de leerling de school verlaten heeft. Er zijn op deze regel echter een aantal uitzonderingen zoals:

- Gegevens over verzuim en in- en uitschrijving: 5 jaar na uitschrijving.
- Gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen: 3 jaar na uitschrijving.

Adresgegevens van (oud-)leerlingen mag de school bewaren bijv. voor het organiseren van reünies.

Kennisnet/PO-raad gaan dit jaar aan de slag om te zorgen dat alle wettelijke bewaartermijnen inzichtelijk worden. De VO-raad geeft dit jaar prioriteit aan het maken van een handleiding voor bewaartermijnen. Dit zal bekend gemaakt worden via de Aanpak IBP (
https://maken.wikiwijs.nl/81891/Informatiebeveiliging___Privacy)
Meer informatie is te vinden op de website van de Autoriteit Persoonsgegevens:
https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/bewaren-van-persoonsgegevens

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

14.18 Model verwerkersovereenkomst versie 3.0.

Dit model is te vinden op: https://www.privacyconvenant.nl/het-convenant/

14.19 Convenant digitale onderwijsleermiddelen.

Dit model is te vinden op Internet:

14.20 Gegevens Functionaris Gegevensbescherming (FG).

Privacy Collectief Theo Kusters, theo@privacycollectief.nl 06 5119 4118

15 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 (wordt op 25-05-2018 vervangen door de AVG).