InformatieBeveiligings- en Privacy beleid

Het Baken Almere
stichting voor interconfessioneel voortgezet onderwijs

IBP v 1.1 | 2019

Inhoud

1 INLEIDING 3

TOELICHTING INFORMATIEBEVEILIGING 3
TOELICHTING PRIVACY 3
VERVLECHTING INFORMATIEBEVEILIGING EN PRIVACY 3

2 DOEL EN REIKWIJDTE 3

DOEL 3
REIKWIJDTE 4

3 UITGANGSPUNTEN 4

ALGEMENE BELEIDSUITGANGSPUNTEN 4
UITGANGSPUNTEN PRIVACY 5

4 WET- EN REGELGEVING 6

5 ORGANISATIE 6

ROLLEN (FUNCTIES) RONDOM IBP 7
RICHTINGGEVEND 7
STUREND 7
UITVOEREND 8

6 CONTROLE EN RAPPORTAGE 8

VOORLICHTING EN BEWUSTZIJN 9
CLASSIFICATIE EN RISICOANALYSE 9
INCIDENTEN EN DATALEKKEN 9
CONTROLE, NALEVING EN SANCTIES 9

BIJLAGEN 10

BIJLAGE 1: PRIVACY STATEMENT 10
BIJLAGE 2: TABEL IBP ROLLEN EN TAKEN 16
BIJLAGE 3: SOCIAL MEDIA POLICY 18
BIJLAGE 4: ICT PROTOCOL VOOR LEERLINGEN 21
BIJLAGE 5: ICT PROTOCOL VOOR MEDEWERKERS 24

1 Inleiding

Het onderwijs 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.

Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.
Deze aspecten zijn:

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

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

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. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een 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.*

Vervlechting informatiebeveiliging en privacy

Informatiebeveiliging is een belangrijk onderdeel 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 Het Baken Almere

2 Doel en reikwijdte

Doel

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van leerlingen, ouders/verzorgers 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 Het Baken Almere voldoet aan relevante wet- en regelgeving.

Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen Het Baken Almere geldt voor alle medewerkers, leerlingen, ouders/verzorgers en externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices (desktop PC's, laptops, telefoons etc.) 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 Het Baken Almere. 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 interne memo's, nieuwsbrieven, uitspraken van medewerkers en leerlingen in discussies en teksten en afbeeldingen op de website.

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Het Baken Almere waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan Het Baken Almere persoonsgegevens verwerkt.

- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van Het Baken Almere 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 Het Baken Almere heeft raakvlakken met:
    - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening (BHV), fysieke toegang en beveiliging, huisvesting en ongevallen
    - Personeelsbeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties, rollen en rechten
    - 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

Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Het Baken Almere zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Algemene Verordening Gegevensbescherming (GDPR).
  De verwerking van persoonsgegevens is gebaseerd op tenminste één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van Het Baken Almere 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 Het Baken Almere 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, data opgeslagen op lokale servers, servers in het datacenter van Veltwerk en data opgeslagen in de Microsoft Cloud (Office365), maar ook van fysieke documenten zoals de papieren leerlingen- en personeelsdossiers, papieren briefwisselingen en handgeschreven memo's.

- 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. Gebruik voor onderwijsdoelstellingen heeft binnen het auteursrecht een speciale plek.

- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij Het Baken Almere geclassificeerd. 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.

- Het Baken Almere 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 leermiddelen privacy' (www.privacyconvenant.nl) en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.

- Er wordt van alle medewerkers, leerlingen, (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. Het Baken Almere heeft hiervoor zijn gedragscodes geformuleerd, vastgesteld en geïmplementeerd voor medewerkers en leerlingen.
  (Bijlage 1)

- Informatiebeveiliging en privacy is bij Het Baken Almere 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 Het Baken Almere vanaf de start rekening gehouden met informatiebeveiliging en privacy. Privacy by default en privacy by design zijn hierbij de standaard.

Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij Het Baken Almere 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.

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 worden adequaat beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van toestemming, zal Het Baken Almere aan de Betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

4 Wet- en regelgeving

Het Baken Almere voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- 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 2.0’ 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 in Het Baken Almere 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.

Rollen (functies) rondom IBP

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Het Baken Almere een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen. (Zie bijlage 2)

Richtinggevend

Eindverantwoordelijke
Het Bevoegd Gezag 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.
De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de Privacy Officer.

Sturend

Privacy Officer (PO)
Privacy Officer is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op uitvoerend niveau. De PO moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen Het Baken Almere
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen Het Baken Almere coördineren

Functionaris voor Gegevensbescherming (FG)
De FG houdt voor Het Baken Almere toezicht op de toepassing en naleving van de AVG. Hij/zij zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten en heeft regelmatig overleg met de PO. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen. De FG doet rechtstreeks verslag aan de Eindverantwoordelijke, het Bevoegd Gezag.

Directeur bedrijfsvoering
Adviseert samen met de PO het Bevoegd Gezag en is medeverantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen Het Baken Almere.

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

Deze proceseigenaar is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties of de data die via de applicatie worden ontsloten. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- Samen met de Privacy Officer stellen zij het beleid voor toegang vast.
- Samen met functioneel beheer en ICT-beheer zien zij er op 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.

Uitvoerend

ICT-beheer
ICT-beheer vormt een technisch aanspreekpunt inzake informatiebeveiliging voor het management en de medewerkers.

Functioneel beheerder
De functioneel beheerder wordt vanuit de domeinverantwoordelijke / proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij/zij zijn of haar taken uit.
.
Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelshandboek, het ICT protocol voor medewerkers en het Social Media protocol. (zie bijlagen)
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 of DR).

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 Privacy Officer.

6 Controle en rapportage

Het informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar 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

Daarnaast hanteert Het Baken een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

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

- **strategisch** niveau richtinggevend wordt gesproken over organisatie en compliance, alsmede over doelen, scope en ambitie op het gebied van IBP.

- **tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.

- **operationeel** niveau worden de onderwerpen besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd, en indien nodig in elk organisatieonderdeel van Het Baken Almere.

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 Het Baken het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en andere stakeholders. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de Privacy Officer met het Bevoegd Gezag als eindverantwoordelijke.

Classificatie en risicoanalyse

Bij Het Baken Almere 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. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang voor de informatievoorziening.

Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij gegevensbescherming@hetbaken.nl. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken. Het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.
(Zie bijlagen)

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 Het Baken wordt actief aandacht besteed aan de AVG bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor de bevordering van de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het Bevoegd Gezag, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het Bevoegd Gezag vast te stellen reglement.

Mocht de naleving ernstig tekort schieten, dan kan Het Baken Almere de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

BIJLAGEN

Bijlage 1: Privacy statement

Privacy statement Het Baken Almere
1. Aanhef

Deze verklaring is voor alle scholen onder het bevoegd gezag van Het Baken Almere waarvan het Bevoegd Gezag gevestigd is te Rooseveltweg 5, 1314 SJ Almere

2. Definities

Persoonsgegevens
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon of kan leiden tot identificatie van een natuurlijk persoon;

Verwerking van Persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

Bijzondere persoonsgegevens
Een persoonsgegeven dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid of zijn gezondheid;

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft al dan niet vertegenwoordigd door diens wettelijk vertegenwoordiger. In dit reglement gaat het om leerlingen en medewerkers;

Wettelijk vertegenwoordiger
Indien de betrokkene de leeftijd van zestien jaren nog niet heeft bereikt, wordt de betrokkene vertegenwoordigd door zijn wettelijk vertegenwoordiger. Meestal zal dit een ouder zijn maar het kan hier ook gaan om een voogd;

Verantwoordelijke
De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Dat wil zeggen de rechtspersoon overeenkomstig de onderwijswetten waar de school onder valt: het bevoegd gezag van Het Baken Almere. Wanneer er in dit regelement gesproken wordt over de verantwoordelijke dan wordt daarmee het bevoegd gezag van alle scholen die behoren tot Het Baken Almere bedoeld.

Bewerker
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

Derde
Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;

3. Reikwijdte en doelstelling

1. Deze verklaring stelt regels op over de verwerking van persoonsgegevens van leerlingen en medewerkers van Het Baken Almere.

2. Deze verklaring is van toepassing op alle persoonsgegevens van de betrokkene die door Het Baken Almere worden verwerkt.

Dit reglement heeft tot doel:

a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens;
b. vast te stellen welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt;
c. de zorgvuldige verwerking van persoonsgegevens te waarborgen;
d. de rechten van betrokkene te waarborgen.

4. Doelen van de verwerking persoonsgegevens

Bij de verwerking van persoonsgegevens houdt Het Baken Almere zich aan de relevante wetgeving waaronder de wet Algemene Verordening Gegevensbescherming (AVG).
De verwerking van persoonsgegevens vindt plaatst voor:

a. het organiseren of het geven van het onderwijs, het begeleiden van leerlingen, dan wel het geven van studieadviezen;
b. het verstrekken of ter beschikking stellen van leermiddelen waaronder ook stage en/of buitenschoolpraktijkleren.;
c. het invullen van de werkgeversrol naar personeel van Het Baken Almere;
d. het bekend maken van informatie over onderwerpen, genoemd onder a, b en c alsmede informatie over de leerlingen, bedoeld in lid a, alsook medewerkers als bedoeld in lid c, op de eigen website;
e. het bekendmaken van de activiteiten van de school op de eigen website;
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 behandelen van geschillen en het doen uitoefenen van accountantscontrole;
h. het onderhouden van contacten met de oud-leerlingen, en/of oud medewerkers van de verantwoordelijke;
i. de uitvoering of toepassing van een andere wet.
j. het aanleveren van persoonsgegevens aan gerelateerde organisaties ten behoeve van analyses en statistische berekeningen.
k. het verkrijgen van leerlinggegevens van de basisschool voor analyse.
l. het leerlingdossier te analyseren en te bespreken met de interne toelatingscommissie een directielid, zorgcoördinator en een orthopedagoog/psycholoog.

5. Gebruik van beeldmateriaal

Gedurende het onderwijstraject van leerlingen van Het Baken Almere kunnen er eventueel foto's en beelden gemaakt worden ten behoeve van in- en extern gebruik ten diensten van het begeleidings- en onderwijsproces van leerlingen. Denk hierbij bijvoorbeeld aan het maken van foto's voor plaatsing op onze website of het maken van beelden/opnames voor een (onderwijs) film van onze school. Voor het gebruik van dit beeldmateriaal worden betrokkenen jaarlijks expliciet om toestemming gevraagd.

6. Vrijstelling meldingsplicht

De in artikel 4 genoemde gegevensverwerkingen vallen onder het vrijstellingsbesluit AVG en hoeven niet worden aangemeld bij de Autoriteit Persoonsgegevens.

7. Doelbinding

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

8. Soorten gegevens

De door de school gebruikte categorieën van persoonsgegevens met betrekking tot leerlingen worden in bijlage 1 van dit Privacy Statement opgesomd.

9. Grondslag verwerking

Verwerking van persoonsgegevens gebeurt alleen op grond van:

a. Toestemming: in het geval de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend
b. Overeenkomst: in het geval de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst
c. Wettelijke verplichting: in het geval de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan Het Baken Almere onderworpen is
d. Vitaal belang.
e. Publiekrechtelijke taak: in het geval de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt
f. Gerechtvaardigd belang.
g. Analyses en statistische berekeningen, in samenwerking met gerelateerde organisaties, ten behoeve voor wetenschappelijk onderzoek.

10. Bewaartermijnen

Het Baken Almere bewaart de gegevens niet langer dan dat zij noodzakelijk zijn voor het vervullen van het doel waarvoor zij zijn verkregen, tenzij er een andere wettelijke verplichting is die het langer bewaren van de gegevens verplicht stelt. De bewaartermijnen zijn vast gelegd in de Dataregisters Leerlingen, Medewerkers en Overige relaties.

11. Toegang

Het Baken Almere, en de daartoe behorende scholen, verlenen slechts toegang tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan:

a. de bewerker en de derde die onder rechtstreeks gezag van Het Baken Almere staat;
b. de bewerker die gemachtigd is om persoonsgegevens te verwerken;
c. derden die op grond van de wet toegang moet worden verleend, waarbij alleen toegang wordt verleend aan de gegevens waartoe volgens de wet toegang toe moet worden gegeven.

12. Beveiliging en geheimhouding

a. Het Baken Almere neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
b. Het Baken Almere en haar scholen zorgen dat medewerkers niet meer inzage of toegang hebben tot de persoonsgegevens dan zij strikt noodzakelijk nodig hebben voor de goede uitoefening van hun werk.

c. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging. Daarbij houdt de school rekening met de concrete risico's die van toepassing kunnen zijn op de verwerkte persoonsgegevens.
d. Iedereen die betrokken is bij de uitvoering van dit reglement, en daarbij de beschikking krijgt over persoonsgegevens die vertrouwelijk zijn of geheim moeten worden gehouden (zoals bijvoorbeeld zorggegevens), en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die persoonsgegevens daarvan.

13. Verstrekken gegevens aan derden

Wanneer daartoe een wettelijke plicht of gerechtvaardigd belang bestaat kan Het Baken Almere de persoonsgegevens verstrekken aan derden. Het verstrekken van persoonsgegevens aan derden kan ook plaatsvinden na toestemming van de betrokkene.

14. Rechten betrokkenen

De AVG geeft de betrokkene een aantal rechten. Het Baken Almere erkent deze rechten en handelt in overeenstemming met deze rechten.

a. **Inzage**
Elke betrokkene heeft recht op inzage van de door Het Baken Almere en de daartoe behorende scholen verwerkte persoonsgegevens die op hem/haar betrekking hebben. Betrokkene kan een afschrift ontvangen van zijn gegevens. Het Baken Almere kan vragen om een geldig identiteitsbewijs ter verificatie van de identiteit van de verzoeker.

b. **Verbetering, aanvulling, verwijdering en afscherming**
Betrokkene kan een verzoeken doen tot verbetering, aanvulling, verwijdering of afscherming van zijn persoonsgegevens, tenzij dit onmogelijk blijkt of een onredelijke inspanning zou vergen, een en ander ter beoordeling door Het Baken Almere.

c. **Verzet**
Voor zover Het Baken Almere persoonsgegevens gebruikt op de grond van de bijlage bij artikel 8 onder e en f, dan kan de betrokkene zich verzetten tegen verwerking van persoonsgegevens op basis van diens persoonlijke omstandigheden.

d. **Termijn**
Het Baken Almere dient binnen een termijn van 4 weken na ontvangst van een verzoek hieraan schriftelijk gehoor te geven dan wel deze schriftelijk, gemotiveerd af te wijzen. Als Het Baken Almere meer tijd nodig heeft om het verzoek te beantwoorden, kan het deze termijn verlengen met maximaal 4 weken.

e. **Uitvoeren verzoek**
Indien het verzoek van de betrokkene wordt gehonoreerd, dragen Het Baken Almere en, indien van
toepassing, de scho(o)l(en) zorg voor het zo spoedig mogelijk doorvoeren van de verzochte wijzigingen.

f. **Intrekken toestemming**
Voor zover voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijde door de betrokkene of diens wettelijk vertegenwoordiger worden ingetrokken.

15. Transparantie

a. Het Baken Almere informeert de betrokkene over de verwerking van zijn persoonsgegevens. Indien het type verwerking dat vraagt, informeert de school iedere betrokkene apart over de details van die verwerking.

b. Het Baken Almere informeert de betrokkene – op hoofdlijnen – ook over de afspraken die gemaakt zijn met derden en bewerkers die persoonsgegevens van de betrokkene ontvangen.

16. Klachten

a. Wanneer u van mening bent dat het doen of nalaten van Het Baken Almere niet in overeenstemming is met de AVG of zoals dat is uitgewerkt in dit reglement is, dan dient u zich te wenden tot Het Baken Almere via **gegevensbescherming@hetbaken.nl**, o.v.v. “klacht uitvoering AVG/privacyreglement”.

b. Overeenkomstig de Wet AVG kan de betrokkene zich eveneens wenden tot de rechter of het College bescherming persoonsgegevens.

17. Onvoorziene situatie

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

18. Wijzigingen reglement

De verantwoordelijke maakt dit reglement openbaar via

- Het Baken Almere openbare website
- Het Baken Almere intranet

De verantwoordelijke heeft het recht dit reglement te wijzigingen. Zodra wij deze privacyverklaring wijzigen zullen wij u binnen een redelijke termijn daarvan op de hoogte brengen. Wij raden u aan de verklaring regelmatig te bekijken om op de hoogte te blijven van de manier waarop we uw persoonsgegevens gebruiken.

19. Slotbepaling

Dit reglement wordt aangehaald als “de privacyverklaring” van Het Baken Almere en treedt in werking op 1 juni 2018.

BIJLAGE 1:

Overzicht van categorieën gebruikte persoonsgegevens m.b.t. leerlingen Indicatie van categorieën Persoonsgegevens die gebruikt kunnen worden:
(lijst is niet limitatief)

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 aard en het verloop van het onderwijs en ondersteuning, alsmede de behaalde studieresultaten;
g. 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);
h. Aanleiding voor de aanmelding bij het samenwerkingsverband, relevante screenings- en onderzoeksgegevens en omschrijving van de problematiek die aan de orde is;
i. Activiteiten die door de school zijn ondernomen rond de betreffende leerling, alsmede de resultaten hiervan;
j. Bestaande of (relevante) afgesloten hulpverleningscontacten en de namen van contactpersonen;
k. Relevante persoonsgegevens die door externe partijen worden verstrekt met betrekking tot de aangemelde problematiek van de betreffende leerling;
l. Relevante financiële gegevens over bijvoorbeeld schoolgeld;

… einde …

Bijlage 2: Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Bevoegd Gezag	• 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 • Het nemen van maatregelen	• Informatiebeveiligings- en privacy beleid • Basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	Privacy Officer Directeur bedrijfsvoering.	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert BG/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 • In overleg met bevoegd gezag melden van een datalek • Evalueren IBP-beleid en maatregelen	Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Bewerkersovereenkomsten 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	• 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 samenspraak met Manager IBP/FG* • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door *Bevoegd Gezag* • *Samen met functioneel beheer en ICT beheer* er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • *Samen met functioneel beheer en ICT* beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• 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

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Uitvoerend (operationeel)	Functionaris gegevensbescherming (VACANT) Uitvoer:DPO	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten.	
		• Uitvoeren taken conform gegeven richtlijnen en procedures.	
	Functioneel beheerder (VACANT) Uitvoer:DPO	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	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
		• Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan.	
	Medewerker	• Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers.	
	Dagelijkse leiding / leidinggevende / directie	• 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.	

… einde …

Bijlage 3: Social Media Policy

maart 2017

Inleiding

Het Baken ziet het gebruik van Sociale Media als een belangrijke maatschappelijke ontwikkeling, met positieve kanten en met mogelijke risico's. In deze Social Media Policy beschrijven we van welke regels elke medewerker en leerling zich bewust moet zijn bij het gebruik van Sociale Media.

Als Sociale Media beschouwen we alle websites waar je met een profiel aanwezig bent en al dan niet geheel of gedeeltelijk transparant, online conversaties kunt hebben. De bekendste Sociale Media sites van dit moment zijn Facebook, Twitter, Linkedin en Youtube. Maar realiseer je dat er elke dag nieuwe bijkomen. Ook sites als bijvoorbeeld Flickr of Slideshare hebben sociale media-achtige aspecten.

Het gebruik

Net zoals bij de opkomst van Internet ontstaan er nieuwe mogelijkheden en is niet meteen duidelijk hoe alles precies geregeld moet worden, maar wij geloven dat elke medewerker en leerling goed in staat is verstandige keuzes te maken. Om hierbij te helpen is dit document opgesteld.

Je gebruikt Sociale Media waarschijnlijk voornamelijk als privépersoon. De formele regels die we hebben, hebben vooral betrekking op wat je doet voor en tijdens schooltijd. Wel vragen we je om ook bij wat je als privépersoon doet, je ervan bewust te zijn dat het steeds makkelijker is voor anderen om te zien wie je bent en waar je naar school gaat. Daarmee ben je ook in wat je in privétijd als privépersoon doet steeds meer ook een vertegenwoordiger van Het Baken.
Wij denken dat als je je daarvan bewust bent, je daar op een verantwoordelijke manier mee zult omspringen.

Tegelijkertijd is het goed je te realiseren dat niet opeens alles nieuw en anders is. Wat hetzelfde blijft is dat je altijd je gezond verstand gebruikt. Realiseer je bijvoorbeeld dat informatie die je op sociale media sites zet eigenlijk niet meer verwijderd kan worden. Ook informatie die je alleen beschikbaar maakt voor "vrienden" kan makkelijk gekopieerd worden en beschikbaar komen voor de rest van de wereld. In de gedragsregels staan veel zaken die ook van toepassing zijn op wat je doet op Sociale Media.

Voor zover je je op sociale media mengt in discussies die direct of indirect gaan over, of te maken hebben met Het Baken, is het goed je te realiseren dat je dan altijd een verantwoordelijkheid hebt als medewerker en als leerling.

Het gebruik van Sociale Media tijdens schooltijd door leerlingen

Leerlingen op Het Baken mogen onder schooltijd (pauzes en na toestemming van de docent) gebruikmaken van sociale netwerken voor privé gebruik, voor zover dat niet ten koste gaat van het werk. Sociale netwerken kunnen ook ingezet worden in lessen of voor school.

Aanwijzingen leerlingen en medewerkers

Bij het gebruik van Sociale Media vragen we je voor zover van toepassing, de volgende aanwijzingen in acht te nemen:

1. Je bent en blijft zelf verantwoordelijk voor wat je communiceert, onder welke naam of alias je dat ook doet. Houd dat altijd in je achterhoofd.

2. Als je accounts of aliassen aanmaakt, is het zonder toestemming van de schoolleiding niet toegestaan Het Baken op enigerlei wijze onderdeel te laten uitmaken van die accountnaam of alias.

3. Voor zover je op sociale media dingen doet / zegt die schadelijk zijn voor Het Baken is er altijd een mogelijkheid dat je daar op wordt aangesproken.

4. Als je iets communiceert dat direct of indirect gaat over Het Baken dan vragen we je nooit negatief te zijn/doen/communiceren; niet over ons en niet namens ons. Voor negatieve communicatie lenen sociale media zich heel slecht en het leidt zelden ergens toe.

5. Als je in een discussie betrokken raakt waarvan je merkt dat die onplezierig wordt, houd er dan mee op in plaats van je te laten meeslepen.

6. Houd er rekening mee dat je in je communicatie geen informatie verspreidt over derden die daar geen toestemming voor hebben gegeven. Bedenk dat steeds meer toepassingen je locatie meesturen en beschikbaar maken voor derden en dat je daarmee dus ook informatie over medewerkers of leerlingen onbedoeld kunt communiceren.

7. Reageer niet impulsief, het kan nooit kwaad twee keer na te denken voordat je een posting doet.

8. Het Baken zal geen ruzies, ontstaan door het gebruik van sociale media in de privésfeer, ‘op gaan lossen’. Het is de verantwoordelijkheid van de gebruiker om zorgvuldig te handelen.

9. Afhandeling van klachten en meldingen van misbruik van sociale media gebeurt volgens de bestaande regels.

We realiseren ons dat de ontwikkelingen op dit gebied razendsnel gaan. In deze regeling hebben we geprobeerd de belangrijkste uitgangspunten en afspraken te vatten, maar volledig kunnen we niet zijn. De belangrijkste afspraak is daarom misschien wel:

Blijf nadenken en houdt het belang van Het Baken altijd in je achterhoofd. Doe normaal!

Bijlage voor medewerkers

1. Medewerkers zijn zich bewust van de voorbeeldfunctie die zij hebben bij het eigen gebruik van sociale media.

2. Medewerkers zijn zich bewust van de rol die zij spelen (vanuit hun verschillende posities op school – mentor, vakdocent) in het signaleren van positief en negatief gedrag van leerlingen bij hun gebruik van sociale media.

3. Medewerkers kennen de positieve en negatieve aspecten van het gebruik van sociale media.

4. Medewerkers stellen zich ten doel een gefundeerde stellingname te kunnen innemen ten opzichte van het gebruik van de sociale media.

5. Medewerkers nemen waar nodig ontwikkelpunten op in hun POP om tot bovenstaand punt 2 en 3 te kunnen komen.

6. Medewerkers erkennen dat het aanleren van de juiste vaardigheden en het juiste gebruik van de sociale media onderdeel moet zijn van het curriculum (en binnen te formuleren leerdoelen) van de school

7. Het gebruik van sociale media moet waarde toevoegen aan de doelstellingen van Het Baken. Het gebruik voor schooldoeleinden moet eraan bijdragen dat jijzelf, collega’s, leerlingen hun werk beter kunnen doen, helpen bij het oplossen van problemen en het verbeteren van vaardigheden en kennis.

8. Bij de geringste twijfel over een publicatie op - of gebruik van sociale media neemt de medewerker contact op met haar / zijn direct leidinggevende

9. Afhandeling van klachten en meldingen van misbruik van sociale media gebeurt volgens de bestaande regels (Zie ook het ICT protocol voor leerlingen / medewerkers)

10. Medewerkers distantiëren zich van deelname aan discussiegroepen zoals Whats-App groepen die door leerlingen zijn opgezet.

11. Medewerkers nodigen geen leerlingen uit tot deelname aan (besloten)discussiegroepen zoals in Whatsapp, Instagram of Facebook.

… einde …

Bijlage 4: ICT protocol voor leerlingen

Gedragscode voor LEERLINGEN
2017

- *We gaan zorgvuldig om met de ICT faciliteiten van de school.*
- *Bij het versturen van berichten gaan we altijd respectvol met elkaar om.*
- *De school controleert de naleving van deze afspraken.*
- *Het niet houden aan afspraken heeft consequenties.*

Uitgangspunten

Op Het Baken vinden we het belangrijk dat we enkel op een zorgvuldige wijze gebruikmaken van ICT-mogelijkheden en middelen. Dit reglement geeft hiervoor de spelregels.
Uitgangspunt vormt daarbij de gewone dagelijkse fatsoensnormen van respectvol met elkaar omgaan. Dit protocol geeft verder richtlijnen voor deskundig en zorgvuldig gebruik van door het Baken ter beschikking gestelde ICT-middelen en draagt zo bij aan een goed en veilig school- en onderwijsklimaat.

Terminologie

Sociale media is een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, inhoud verzorgen, publiceren en delen.
Een aantal voorbeelden hiervan zijn WhatsApp, Facebook, Tumblr, Instagram, YouTube en Snapchat. E-mailverkeer is ook een middel tot het verspreiden en delen van berichten. In het kader van dit protocol wordt e-mailverkeer daarom veronderstelt onderdeel uit te maken van het verzamelbegrip sociale media.

Doelgroep

Deze regeling is van kracht voor alle leerlingen van Het Baken en leerlingen die in het kader van uitwisselingsprogramma's tijdelijk gebruikmaken van de ICT faciliteiten van de Bakenscholen.

ICT-protocol voor leerlingen van Het Baken

1. Algemene uitgangspunten computergebruik

Iedere leerling is verantwoordelijk voor de hard-/software waarmee van het netwerk van de school gebruik wordt gemaakt. In het besef dat je gebruik maakt van andermans spullen, doe je dit zorgvuldig en netjes. Wat niet mag is:

- Laat geen andere mensen werken op jouw account.
- Werk nooit op het account van een ander.
- Laat nooit jouw computersessie openstaan wanneer je weg loopt bij je computer.
- Geef nooit je persoonlijke user-id en wachtwoord aan anderen.
- Indien het vermoeden bestaat dat anderen op de hoogte zijn van je wachtwoord, maak dan zo snel mogelijk een nieuw wachtwoord.
- Het is niet toegestaan zonder toestemming bestanden te downloaden van het internet
- Het is zonder toestemming niet toegestaan programma's op de computer te instaleren
- Het is zonder toestemming niet toegestaan systeeminstellingen op de computer te wijzigen.

2. Waarom afspraken voor het gebruik van sociale media?

Sociale media zijn door toegankelijkheid en gebruik vatbaar voor misbruik.
Van belang is te beseffen dat je met berichten op sociale media (onbewust) de goede naam van personen kunt schaden. Dat willen we niet en dat mag ook niet.

De controle op het delen van persoonsgegevens via sociale media heeft als doel:

- Het leveren van bewijsvoering bij misbruik.
- Het tegengaan van berichten die op enige wijze aanstootgevend kunnen zijn of personen kunnen schaden; in het bijzonder geldt:

  - Geen kwetsend of grof taalgebruik
  - Geen scheldpartijen
  - Geen persoonlijke aanvallen
  - Geen discriminerende, racistische of seksistische bijdragen
  - Geen pornografische teksten
  - Geen seksuele intimidatie
  - Geen commerciële boodschappen

4. Internetgebruik

Internetgebruik op school is vooral bedoeld om bij te dragen aan het leerproces. Alles wat behoort tot het vervullen van opdrachten vanuit de school is dus toegestaan.
Je houdt daarbij rekening met de volgende belangrijke regels:

- Ook voor het gebruik van het internet gelden de normale algemene fatsoensnormen.
- Je schendt de auteursrechten van derden niet
- Je bezoekt geen sites die pornografisch, racistisch, discriminerend, beledigend, geweldadig of aanstootgevend materiaal bevatten
- Zonder toestemming is het downloaden en opslaan van bestanden niet toegestaan.

Wanneer je je aan bovengenoemde afspraken houdt, is het toegestaan om het internet voor persoonlijke doeleinden te gebruiken mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.

5. Controle

Controle op alles wat in dit protocol is omschreven als 'verboden of tegengaan' vindt plaats door:

- Vastlegging van je computergebruik d.m.v. automatische logbestanden
- Geautomatiseerd terugsturen van verdachte berichten naar afzender
- Het blokkeren van verboden sites
- Het doorgeven van misbruik aan mentor en ouders/verzorgers door de schoolleiding
- Ter bewijsvoering het zonder mededeling vooraf inzien van berichten en bestanden door de schoolleiding

6. Wat gebeurt als je je niet aan afspraken houdt?

- Je wordt aangesproken op je gedrag
- Als de overtreding ernstig is kun je een officiële waarschuwing krijgen
- Het blokkeren van de toegang tot (alle) ICT-faciliteiten.
- Bij een herhaling bestaat de mogelijkheid dat je van school wordt verwijderd
- Afhankelijk van de ernst van het voorval, aangifte bij politie Ouders/verzorgers en de meerderjarige leerling worden aansprakelijk gesteld voor kosten en schade

7. Rechten en plichten

- De school houdt zich aan de bepalingen in de Wet Bescherming Persoonsgegevens: https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/inhoud/bescherming-persoonsgegevens
- De schoolleiding informeert de ouders/verzorgers en leerlingen en medewerkers voorafgaand aan de invoering van deze regeling
- De regeling verlangt instemming van de medezeggenschapsraad, evenals toekomstige wijzigingen

8. Slotbepaling

- Als zich situaties voordoen waarin deze regeling niet voorziet, zal de bestuurder na advies ingewonnen te hebben bij de medezeggenschapsraad, handelen.
- De algemene regels en normen die van kracht zijn in de omgang tussen mensen, gelden ook bij het gebruik van e-mail en internet.

… einde …

Bijlage 5: ICT protocol voor medewerkers

Gedragscode voor MEDEWERKERS
2017

- *We gaan zorgvuldig om met de ICT faciliteiten van de school.*
- *Bij het versturen van berichten gaan we altijd respectvol met elkaar om.*
- *Je bent je bewust van de beveiligingsrisico's bij het beheren van persoonsgegevens.*

Uitgangspunten

- Het Baken en de onder haar bevoegd gezag ressorterende scholen voor voortgezet onderwijs (te noemen: de scholen) onderkennen het belang van communicatie via e-mail en sociale media en de waarde van de hiervoor beschikbaar gestelde faciliteiten.
- Dit protocol bevordert dat de medewerkers en leerlingen, bij uitingen via e-mail en sociale media, communiceren in overeenstemming met de reguliere fatsoensnormen en, voor zover het medewerkers betreft, in overeenstemming met de visie en missie van de scholen. Dit betekent onder meer dat we respect hebben voor de scholen en elkaar, en dat we iedereen in zijn waarde laten.
- Het protocol dient de scholen, haar medewerkers, leerlingen en ouders/verzorgers van de leerlingen te beschermen tegen de mogelijke negatieve gevolgen van sociale media en e-mailgebruik.
- Dit protocol geeft richtlijnen voor deskundig en zorgvuldig gebruik van door het Baken ter beschikking gestelde ICT-middelen.
- Dit protocol draagt bij aan een goed en veilig school- en onderwijsklimaat.

Terminologie

Sociale media is een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, inhoud verzorgen, publiceren en delen.
Een aantal voorbeelden hiervan zijn WhatsApp, Facebook, Tumblr, Instagram, YouTube en Snapchat. E-mailverkeer is ook een middel tot het verspreiden en delen van berichten. In het kader van dit protocol wordt e-mailverkeer daarom veronderstelt onderdeel uit te maken van het verzamelbegrip sociale media.

Doelgroep

Deze regeling is van kracht voor alle werknemers van Het Baken, zowel intern als extern. Externe medewerkers zijn onder andere stagiairs, uitzendkrachten, consultants enz.

---

1. Sociale media* en internet (*zie voor verdere regelgeving "Social Media Policy van Het Baken")

De algemene regels en normen die van kracht zijn in de omgang tussen mensen, gelden ook bij het gebruik van sociale media en internet. Sociale media en internet zijn door toegankelijkheid en gebruik vatbaar voor misbruik. Dat willen we niet, dat mag ook niet. Daarnaast worden er (maatschappelijke, wettelijke) eisen gesteld aan het gedrag van onderwijsorganisaties en in het bijzonder van medewerkers. Dan is er nog het risico van systeembeschadigingen, we willen dat het systeem soepel blijft functioneren.
De controle op het delen van persoonsgegevens via sociale media heeft als doel:

- Het leveren van bewijsvoering bij misbruik.
- Het tegengaan van berichten die op enige wijze aanstootgevend kunnen zijn of personen kunnen schaden; in het bijzonder geldt:
  - Geen kwetsend of grof taalgebruik
  - Geen scheldpartijen
  - Geen persoonlijke aanvallen

- Geen discriminerende, racistische of seksistische bijdragen
- Geen pornografische teksten
- Geen seksuele intimidatie
- Geen commerciële boodschappen

2. Computergebruik

Iedere medewerker is verantwoordelijk voor de hard-/software waarmee van het netwerk van de school gebruik wordt gemaakt. In het besef dat je gebruik maakt van andermans spullen, doe je dit zorgvuldig en netjes. Wat niet mag is:

- Laat geen andere mensen werken op jouw account.
- Werk nooit op het account van een ander.
- Laat nooit jouw computersessie open staan wanneer je weg loopt bij je computer.
- Geef nooit je persoonlijke user-id en wachtwoord aan anderen.
- Indien het vermoeden bestaat dat anderen op de hoogte zijn van je wachtwoord, maak dan zo snel mogelijk een nieuw wachtwoord.
- Laat opslag media zoals USB-stick en portable harddisks niet onbeheerd achter
- Laat handheld devices zoals mobiele telefoon, tablet op laptop niet onbeheerd achter.

3. E-mailgebruik

Richtlijnen voor e-mailberichten:

- Maak persoonlijke e-mailberichten herkenbaar door middel van het woord *privé* in de onderwerpregel.
- Onderteken bij persoonlijke e-mailberichten als privé-persoon, dus met weglating van functie, afdeling, naam van de school en logo.
- Sluit zakelijke e-mailberichten af met je eigen naam, Het Baken en afdeling en telefoonnummer (indien aanwezig: bij voorkeur je eigen doorkiesnummer).
- Op basis van de capaciteit van het systeem zijn er grenzen gesteld aan de omvang van bijlagen.

4. Internetgebruik

Voor het gebruik van het internet gelden de normale algemene fatsoensnormen. Daarnaast geldt:

- Je schendt de auteursrechten van derden niet.
- Je bezoekt geen sites die pornografisch, racistisch, discriminerend, beledigend, geweldadig of aanstootgevend materiaal bevatten

Wanneer je je aan bovengenoemde afspraken houdt, is het toegestaan om het internet voor persoonlijke doeleinden te gebruiken mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.

5. Controle

Alleen bij zwaarwegende redenen vindt er controle plaats.
Controle op alles wat in deze regeling is omschreven als 'verboden of tegengaan' vindt plaats door:

- Geautomatiseerd terugsturen van verdachte berichten naar afzender
- Het blokkeren van verboden sites
- Ter bewijsvoering zonder mededeling vooraf inzien van berichten en bestanden
- Uitlezen van je computergebruik middels logbestanden

Bij een redelijk vermoeden van een strafbaar feit kan het bestuur besluiten tot het inzage nemen van het berichtenverkeer van betrokkenen. Het bestuur zal hiervan achteraf melding doen en verklaring afleggen bij het dagelijks bestuur van de MR en bij de vertrouwenspersoon.

6. Wat gebeurt als je je niet aan de afspraken houdt?

Medewerkers die in strijd handelen met dit protocol maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het personeelsdossier.

Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen:

- Worden rechtspositionele maatregelen genomen conform de dan geldende cao voor het voortgezet onderwijs
- Wordt de toegang tot (alle) ICT-faciliteiten geblokkeerd
- Zal aangifte bij de politie worden gedaan
- Wordt de werknemer aansprakelijk gesteld voor kosten en schade

7. Beheer van persoonsgegevens; melding van datalek

Medewerkers zijn persoonlijk verantwoordelijk voor het veilig en zorgvuldig beheer van de persoonsgegevens van leerlingen, ouders en medewerkers waar zij uit hoofde van hun functie en taken beschikking over krijgen.
Wanneer een medewerker een beveiligingsincident constateert waarbij mogelijk sprake is van een datalek, is de medewerker verplicht dit direct te melden bij de directeur/rector van de school. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs is uit te sluiten.

- Het kwijt raken van USB stick, telefoon, laptop
- Onzorgvuldig handelen (bv het plaatsen van gevoelige data op een openbare plek. Het verzenden van data naar personen die over deze data niet mogen beschikken)
- Geconstateerde of vermoede diefstal van USB stick, telefoon, laptop
- Inbraak door hacking

8. Rechten en plichten

- De school houdt zich aan de bepalingen in de Wet Bescherming Persoonsgegevens: https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/inhoud/bescherming-persoonsgegevens
- De schoolleiding informeert de medewerkers over de invoering van deze regeling.
- De regeling verlangt instemming van de medezeggenschapsraad, evenals toekomstige wijzigingen.

9. Slotbepaling

- Als zich situaties voordoen waarin deze regeling niet voorziet, zal de bestuurder na advies ingewonnen te hebben bij de medezeggenschapsraad, handelen.
- De algemene regels en normen die van kracht zijn in de omgang tussen mensen, gelden ook bij het gebruik van e-mail en internet

… einde …