concept
Informatie Beveiligings- en Privacybeleid

St. Brevoordt

Ingangsdatum	: 1 mei 2018
Opgesteld door	: A. Kreunen
Vastgesteld op	:

1 Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ict. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ict en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk 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.

2 Toelichting informatiebeveiliging en privacy

2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:
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 ongewenste risico's in het uitvoeren van de taken van de stichting en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

2.2 Toelichting privacy

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

2.3 Vervlechting informatiebeveiliging en privacy

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

3 Doel en reikwijdte

3.1 Doel

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

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en dat de Stichting Brevoordt voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen Stichting Brevoordt geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het instellingsnetwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting Brevoordt waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting Brevoordt persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting Brevoordt. Hieronder valt tevens de gecontroleerde informatie, die door de instelling zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de instelling kan worden aangesproken. (b.v. uitspraken van medewerkers in discussies, op (persoonlijke pagina's van) websites en of sociale media.)
- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Stichting Brevoordt evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- IBP-beleid heeft binnen Stichting Brevoordt raakvlakken met:
  - . *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen. De stichting Brevoordt sluit wat betreft deze aspecten aan op het Algemeen veiligheids- en toegangsbeveiligingsbeleid van St. De Korenburg, waarvan zij de werkruimtes en digitale omgeving huurt.
  - . *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. Ook dit is geborgd in de samenwerking met St. De Korenburg.
  - . *Medezeggenschap.*

4. Beleid; de uitgangspunten

Stichting Brevoordt hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het bestuur van Stichting Brevoordt neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
2. Stichting Brevoordt voldoet aan alle relevante wet- en regelgeving.
3. Bij Stichting Brevoordt is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Stichting Brevoordt om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens, is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen altijd hun toestemming herzien.
4. Stichting Brevoordt zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
5. Stichting Brevoordt legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Stichting Brevoordt voldoet hiermee aan de documentatieplicht.
6. Binnen Stichting Brevoordt 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 papieren documenten.
7. Stichting Brevoordt is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de instelling informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. Stichting Brevoordt classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de tenemen maatregelen.
9. Stichting Brevoordt sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de stichting, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
10. Stichting Brevoordt verwacht van alle medewerkers, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Stichting Brevoordt heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij Stichting Brevoordt een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing

gewenst is.

12. Stichting Brevoordt kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.
13. Stichting Brevoordt neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.
    Voor dat deel van de infrastructuur dat elders wordt beheerd en/of gegevens elders worden verwerkt legt Stichting Brevoordt aanvullende afspraken vast over de technische maatregelen.
14. Stichting Brevoordt zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

5. Uitwerking van het beleid

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

5.1 Relevante wet- en regelgeving

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

- Wet op het primair onderwijs
- Wet goed onderwijs en goed bestuur PO
- Wet Bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

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

5.2 Basisregels bij het omgaan met persoonsgegevens

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

1. ***Doelbepaling en doelbinding**:* persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. ***Grondslag**:* verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
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 (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. ***Transparantie**:* de stichting legt aan betrokkenen (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 betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. ***Data-integriteit**:* er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

5.3 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

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

5.5 Classificatie en risicoanalyse
Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.6 Incidenten en datalekken
Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij de directeur van de Stichting Brevoordt. Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7 Planning en controle
Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

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

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

5.8 Naleving en sancties
De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan Stichting Brevoordt de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.9 Logging en monitoring

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

6 Organisatie

6.1 Rollen en verantwoordelijkheden

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. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij Stichting Brevoordt.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Bestuur	Eindverantwoordelijk IBP-beleidsplan	Vaststelling IBP-Beleidsplan
	Directeur-bestuurder	IBP-beleidsvorming, -vastlegging en het uitdragen ervan Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens Evalueren toepassing en werking IBP-beleid op basis van rapportages Organisatie IBP inrichten	Informatiebeveiligings- en privacy beleid Basismaatregelen Reglement FG vaststellen Privacyreglement vaststellen
Sturend (tactisch)	Directeur-bestuurder	Inhoudelijk verantwoordelijk voor IBP IBP-planning en controle Adviseert bestuur 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 beeldmateriaal Opstellen informatie documentatie richting leerlingen, ouders / verzorgers Security awareness activiteiten Sociale media reglement Gedragscode ict en internetgebruik Gedragscode medewerkers
	Functionaris voor Gegevensbescherming	Toezicht op naleving privacy wetgeving Voorlichting privacy en stimuleren bewustwording Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens Incidentafhandeling (registreren en evalueren). Technisch aanspreekpunt voor IBP-incidenten.	Privacyreglement, procedure IBP-incident afhandeling Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.: ICT, administratie	**Classificatie / risicoanalyse** in samenwerking met directeur Toegangsbeleid zowel fysiek als digitaal vaststellen Samen met directeur en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek	Inventariseren waar persoonsgegevens van de St. Brevoordt terechtkomen (leveranciers lijst); input dataregister Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen,

		bevoegd zijn. Samen met directeur en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	waaronder: Toegangsmatrix diverse informatiesystemen en netwerk
Uitvoerend (operationeel)	Functioneel en/of applicatie beheerder Medewerker Directeur-bestuurder	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

De verdere uitwerking van de rollen en taken staan beschreven in bijlage 2.

7 De invulling en uitvoering

7.1 Controle en rapportage

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur van het stichting.
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 kent de stichting Brevoordt een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarbij de inhoud en effectiviteit van het IBP-beleid wordt getoetst (bijlage 3).

7.2 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 het bewustzijn van de individuele medewerkers binnen de stichting 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/voorlichting voor medewerkers, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de directeur en de ICT-coördinator.

7.3 Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij de leidinggevende en bij ***privacy@brevoordt.nl*** Een incident dat kan leiden tot een datalek is bijvoorbeeld de diefstal van een laptop of telefoon met persoonsgegevens. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Een datalek wordt gecommuniceerd naar betrokken instanties en partijen. Een medewerker is verplicht binnen 72 uur een datalek te melden bij de Autoriteit Persoonsgegevens.
Bovenstaande is beschreven in een protocol. Dit protocol is als bijlage toegevoegd (bijlage 4).

7.4 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 medewerkers hun verantwoordelijkheid nemen en alkaar aanspreken in geval van tekortkomingen. Bij de St. Brevoordt wordt actief aandacht besteed aan IBP bij de benoeming van medewerkers en tijdens functioneringsgesprekken. De professionele houding van de medewerker ten opzichte van de Informatie Beveiliging en Privacy is voortdurend onderwerp van gesprek.
Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens en zijn opvolger de AVG, vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de directeur-bestuurder. Hij heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.
Mocht de naleving van de afspraken conform het IBP-beleid ernstig tekort schieten, dan kan de St. Brevoordt de betrokken verantwoordelijke medewerkers een disciplinaire-maatregel op leggen. Dit binnen de kaders van de CAO en de wettelijke mogelijkheden.

7.5 Databeveiliging en continuïteit

Eigen gebruikersaccount
Iedere medewerker van het netwerk binnen de St. Brevoordt ontvangt zijn of haar eigen gebruikersaccount. De inloggegevens hiervoor zijn privé en mogen niet worden gedeeld. Aan het

gebruikersaccount is een Brevoordt-emailadres gekoppeld. Dit emailadres wordt te allen tijde gebruikt voor communicatie richting interne- en externe partijen.

Personeelsdossiers
De personeelsdossiers zijn wat betreft de salarisgegevens gedigitaliseerd en beschikbaar in het personeelsadministratiesysteem van O.B.T. Aan alle medewerkers is een uniek wachtwoord verstrekt en alle nieuwe medewerkers ontvangen bij hun aanstelling rechtstreeks een wachtwoord voor OBT.
De directie is verantwoordelijk voor het personeelsdossier van elke medewerker. De dossiers zijn digitaal geborgd en beveiligd in een aparte map. Het papieren dossier is opgeborgen in een afgesloten dossierkast.
Bewaartermijnen van privacygevoelige personeelsinformatie: voor alle medewerkers worden de persoonlijk personeelsdocumenten bewaard gedurende de periode dat ze voor de St. Brevoordt werkzaam zijn. Een jaar na vertrek wordt het hele personeelsdossier vernietigd, tenzij er en beargumenteerde reden is om het dossier langer te bewaren. Dat wordt dan schriftelijk aan de desbetreffende medewerker meegedeeld.

Wanneer rechtspositionele aspecten in het geding zijn, kunnen gegevens uit het personeelsdossier naar buiten gebracht worden. De beoordeling en verantwoordelijkheid daartoe berust bij de directeur.

Wachtwoorden
Het wachtwoord behorende bij het gebruikersaccount moet verplicht 1x per half jaar worden aangepast en moet voldoen aan complexiteitseisen. In de (interne) notitie ‘Werkvoorschriften gebruik digitale apparatuur’ staan de eisen aan de wachtwoorden uitgewerkt. Naleving en controle vallen on der de verantwoordelijkheid van de directeur.

Opslaan van gegevens
Binnen de stichting wordt er gebruik gemaakt van Microsoft Office. Alle gegevens worden opgeslagen op de eigen centrale server met alleen geautoriseerde toegang door de medewerkers binnen de St. Brevoordt.

De ICT-coördinator regelt de toegang tot de data.
Het opslaan van bestanden op gebruikersapparatuur van de stichting of van medewerkers is niet toegestaan. Zo wordt schade bij verlies of diefstal beperkt.
Het is niet toegestaan om privacygevoelige informatie op te slaan op een externe gegevensdrager zoals een usb drive of cd-rom. Ook opslag van deze informatie op werkstations/telefoons/tablets van medewerkers is zonder een extra beveiligingslaag niet toegestaan.

Delen van gegevens
Het delen van privacygevoelige informatie gebeurt alleen binnen de doelen en geregistreerde medewerkers van de stichting. Delen van privacygevoelige informatie aan derden is niet toegestaan zonder aantoonbare schriftelijke toestemming van betrokkenen. Bij het delen van data gaan we ervan uit dat we hierbij zelf eigenaar blijven.
Alle partijen waarmee we data delen die betrekking heeft op persoonsgegevens moeten voldoen aan het privacy convenant zoals is opgesteld door de PO-raad. Hierbij moet worden aangegeven welke gegevens worden gebruikt en waarom. Daarnaast wordt hierin ook aangegeven hoe de betreffende partij omgaat met incidenten en beveiliging van de data. Deelnemende partijen zijn in te zien op: https://www.privacyconvenant.nl/de-deelnemers/

Indien een partij niet is aangesloten moet er een aparte overeenkomst worden opgesteld waarin alle afspraken staan benoemd. Hiervoor is een modelovereenkomst verkrijgbaar op de website van het platform. Meer informatie over het convenant en een modelovereenkomst zijn terug te vinden op: https://www.privacyconvenant.nl/het-convenant/

Werkplekken en apparatuur
De apparatuur die tot beschikking wordt gesteld aan medewerkers is voorzien van een virusscanner die zorgt voor een adequate beveiliging.
De apparatuur die beschikbaar is gesteld door de stichting is optimaal beveiligd. Het gebruik van eigen smartphones kan alleen als er door de ICT-beheerder van de stichting aangegeven is dat het device op de juiste beveiligd is en zodanig ingericht is dat er contact kan worden gelegd met de beveiligde server-omgeving.
De eindverantwoordelijkheid hiervoor ligt bij de directeur, de technische uitvoering bij de ict-beheerder.
Bij het verlaten van een werkplek moet deze worden vergrendeld, zodat deze niet toegankelijk is voor derden.

Back-ups van bestanden
Alle bestanden worden opgeslagen binnen de server van de stichting. Elke nacht wordt er automatisch een back-up gemaakt. Die back-up wordt bewaard op een veilige plek buiten het gebouw waar de server staat.

Websites en social media
Persoonsgegevens van leerlingen worden in principe niet op de website geplaatst.
Voor gebruik van foto's op de website van de stichting is het van belang dat er jaarlijks schriftelijke toestemming van de ouders is verkregen. Ouders zijn jaarlijks schriftelijk op de hoogte gesteld van het feit dat zij deze toestemming ook te allen tijde weer kunnen intrekken.
Toestemming voor het plaatsen van foto's op de website is nog geen toestemming om deze ook te plaatsen op social media (bijvoorbeeld Facebook) of in andere documenten. Hiervoor wordt apart jaarlijks schriftelijk toestemming voor gevraagd. Ouders worden tevens jaarlijks schriftelijk op de hoogte gebracht van het feit dat zij deze toestemming te allen tijde weer kunnen intrekken.

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Verplicht vanuit de AVG:

Procesbeschrijving melden datalekken		gereed
Registratie beveiligingsincidenten		gereed
Dataregister om te voldoen aan de registratieplicht		gereed
Verwerkersovereenkomsten		gereed
Procedure gegevensbeschermingseffectbeoordeling (DPIA)		klaar per 01-10-2018
Risicoanalyse		klaar per 01-12-2018
Functionaris voor Gegevensbescherming	Functie beleggen	benoemd per 01-01-2019

Verdere documenten:

Procedure voor verwijderen van gegevens	(w.o. bewaartermijnen)	klaar per 1-10-2018
Communicatie rechten betrokkenen	(protocol)	klaar per 01-12-2018
Procesbeschrijving rechten betrokkenen	(protocol rondom aanvragen van betrokkenen)	klaar per 01-12-2018
Privacyreglement		gereed
Autorisatiematrix	(wie mogen gegevens inzien, bewerken enz.)	klaar per 01-10-2018
Afspraken gebruik sociale media		gereed
Procedure rondom training medewerkers	(bewustzijn creëren)	gereed
Werkvoorschriften gebruik digitale apparatuur	(w.o. wachtwoordbeleid)	gereed per 25-06-2018
Gedragscode ict en internetgebruik		
Procedure rondom uitwisselen gegevens	(passend onderwijs, leerling, dossiers, enz)	klaar per 01-10-2018

Bijlage 2: Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.
Richtinggevend (strategisch)
Sturend (tactisch)
Uitvoerend (operationeel)
Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Stichting Brevoordt voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.
Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Eindverantwoordelijke
Het bestuur is eindverantwoordelijk voor IBP en stelt het beleid op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd.
Het maken van het beleid en de inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de directeur.

Sturend

De directeur is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De directeur moet:
Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
De uniformiteit bewaken binnen Stichting Brevoordt.
Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
De verdere afhandeling van incidenten binnen Stichting coördineren

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG) houdt binnen Stichting Brevoordt 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 verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het bestuur). De FG heeft regelmatig overleg met de directeur. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen. De FG is het technisch aanspreekpunt voor IBP-incidenten en zorgt voor het registreren en evalueren van incidenten.

Domeinverantwoordelijken
Binnen de stichting zijn er verschillende domeinen zoals ict en secretariaat. Op elk van deze domeinen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven en uitgevoerd.
Deze domein-/proceseigenaar is tevens 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 de directeur stellen zij het beleid voor toegang (autorisaties) vast.
Samen met ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
Samen met de directeur en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

Uitvoerend

Applicatiebeheerder (ICT-beheerder)
Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De ICT beheerder wordt vanuit de domeinverantwoordelijke / proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.
.
Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. De medewerkers zijn geschoold in het handelen binnen het IBP-beleid en worden 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.

Leidinggevende
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. De directeur heeft op uitvoerend niveau de taak om:
er voor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid;
toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.
De leidinggevende kan in zijn taak ondersteund worden door de manager IBP. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Bijlage 3 Planning en control; een risico-analyse

Om risico's in beeld te krijgen voert de stichting jaarlijks een risicoanalyse m.b.v. een workshop uit. Tijdens de risicoanalyse worden eerst de risico's bepaald en daarna worden de maatregelen die nodig zijn om die risico's tot een minimum te beperken bepaald.
Een risicoanalyse zal niet alleen de grootste risico's aan het licht brengen, zodat je weet waar je als eerste in moet investeren. Het is ook een middel om te zorgen dat iedereen hetzelfde beeld krijgt over risico's en de nadelige gevolgen voor de school. Denk bij nadelige gevolgen aan:

1. Reputatieschade: door incidenten die gemeld worden in de media. Bijvoorbeeld examenfraude, wachtwoorden op straat, gestolen examens. Dit is slecht voor het imago van de stichting.
2. Financiële schade: als leerling gegevens niet juist zijn kan de bekostiging van deze leerlingen in gevaar komen; je niet houden aan de privacywetgeving kan financiële consequenties hebben, zoals het niet melden van een datalek.
3. Continuïteit het onderwijs: Cybercrime en DDos-aanvallen kunnen het werk binnen de stichting enorm verstoren.
4. Wet en regelgeving: er moet aantoonbaar voldaan worden aan de AVG.
5. Risico's in de cloud: toepassingen in de cloud leveren specifieke aandachtspunten op zoals eigenaarschap, toegang, privacy en continuïteit van de dienstverlening van externe partijen.
6. Te beperkt kennisniveau: ontwikkelingen gaan snel, de eisen om te voldoen aan wet- en regelgeving worden strenger en de risico's groter. Onvoldoende kennis kan tot gevolg hebben dat er onjuiste beslissingen worden genomen ten aanzien van informatiebeveiliging en privacy met alle gevolgen van dien.

Bijlage 4 Protocol incidenten en datalekken

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van de stichting.
Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken.

Gebruikte termen
Beveiligingsincident. Een beveiligingsincident is een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
Informatievoorziening. Het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
Datalek. Een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, etc.) Alle datalekken zijn beveiligingsincidenten maar niet alle beveiligingsincidenten zijn datalekken.
Betrokkene De persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken
Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplichting melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete.
De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Als gebruik maakt van andere partijen, zoals een administratiekantoor, die persoonsgegevens ontvangen van de school, dan moet de school met deze bewerkers aanvullende afspraken over het melden van datalekken.
Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan óf waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie ‘gelekt’. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop het verslag van een leerling, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het bestuur van de St. Brevoordt. Een leverancier is een bewerker voor de school. Er kan worden afgesproken dat een bewerker namens de verantwoordelijke de melding doet maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur. Dat moet wel worden afgesproken anders zal de verantwoordelijke zelf de melding moeten doen.
Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.
Het stichting maakt als verantwoordelijke voor de persoonsgegevens afspraken maken met andere partijen (verwerkers) als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder.

- Hoe informeer je elkaar over datalekken, en zorg ook voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatie gegevens de bewerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding (maak afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de bewerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

Voor de schriftelijke afspraken met de bewerker(s) maken we gebruik van het model bewerkersovereenkomst bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).

Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid;
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen en/of gedragscode ict en internetgebruik.

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1. Ontdekker (medewerker); degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. Meldpunt (servicedesk); een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. Melder (functionaris gegevensbescherming); degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. Technicus (ict coördinator); degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De zeven stappen:

1. Ontdekken

De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het meldpunt via privacy@swvoostachterhoek.nl

2. Inventariseren

Het Meldpunt bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd:
Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
Datum/periode van het beveiligingsincident
Aard van het beveiligingsincident
Wanneer van toepassing (bij een datalek):
Omschrijving van de groep betrokkenen
Aantal betrokkenen
Type persoonsgegevens in kwestie
Worden de gegevens binnen een keten gedeeld

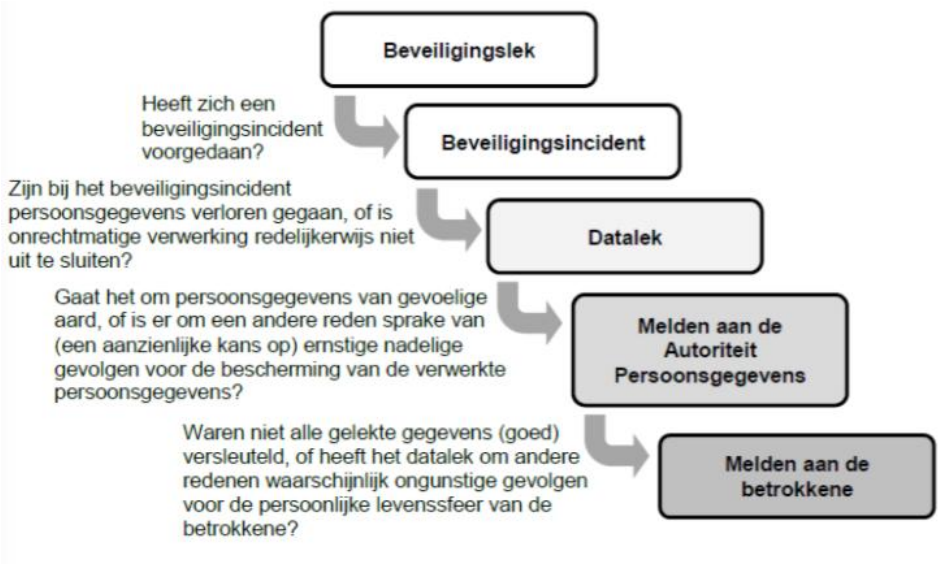
3. Beoordelen

Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoedt, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.
De volgende informatie wordt vastgelegd door de Melder:
Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen;

Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
Wordt het datalek aan betrokkenen gemeld? Waarom niet?
Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

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

Onderstaande beslisboom kan gebruikt worden



4. Repareren

De technicus, de ICT-medewerker, wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De ICT-medewerker van de St. Brevoordt legt onderstaande vast:
Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

5. Melden

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0. Het meldingsformulier is openbaar en neem eens een kijkje welke informatie er eigenlijk nodig is om een datalek te melden. Dan ben je voorbereid als dat ooit nodig mocht zijn.

6. Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident is afgesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

7. Informeren betrokkene: leerling en/of zijn ouders

Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan er van worden uitgaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.