SCHOLENGEMEENSCHAP
Scholen met de Bijbel
IPCO · NaPCO VZW

INFORMATIEVEILIGHEID- EN PRIVACYBELEID

vzw SmdB De Springplank

voor:

SmdB De Springplank

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-03-05	werkdoc	Jasper Vanwalleghem	Markering: invullen school/ instelling/ bestuur adhv 'zoek & vervang' Markering: te bespreken
1.1	2018-03-06	werkdoc	Jasper Vanwalleghem	Toepassen lay-out huisstijl IPCO
1.2	2018-05-15	werkdoc	Jasper Vanwalleghem	Uniformiseren wijzigingen #...#
1.3	2018-07-01	werkdoc	Jonathan De Laet Karolien Deraeve	Invullen variabelen, aanpassen naar onze situatie
1.4	2018-08-25	publiek	Jonathan De Laet	Klaarmaken voor publicatie

Inhoudsopgave

1 INLEIDING

Informatie en ict zijn noodzakelijk in de ondersteuning van het onderwijs. Denken we maar aan de leerlingadministratie- en leerlingvolgsystemen, agenda- en rapportprogramma's, oefen- en toetssystemen…. Vaak verwerken deze geautomatiseerde systemen persoonsgegevens (van leerlingen, ouders, lesgevers…) en is de privacywetgeving (AVG) hierop van toepassing.

Deze informatieverwerking en het gebruik van ict brengen risico's met zich mee. Denken we bijvoorbeeld maar aan een cyberaanval waarbij de gegevens versleuteld worden, een vergissing waardoor gegevens onherroepelijk gewist zijn, de natuur (bijv. overstroming of brand), et cetera. Het niet beschikbaar zijn van ict, incorrecte administraties en het uitlekken van gegevens kan leiden tot inbreuken op het geven van onderwijs en het vertrouwen in onze school.

Deze bedreigingen maken het noodzakelijk om adequate maatregelen te nemen op het gebied van informatieveiligheid en privacy (IVP) om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Om dit structureel op te pakken is het noodzakelijk dat we duidelijk maken waar het om gaat, welk doel we stellen en de manier waarop we dit doel willen bereiken.

1.1 TOELICHTING INFORMATIEVEILIGHEID

Onder informatieveiligheid wordt verstaan: het nemen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatie en ICT zo maximaal mogelijk te garanderen.

Deze kwaliteitsaspecten zijn:

- **Beschikbaarheid:** de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- **Integriteit:** de mate waarin gegevens en/of functionaliteiten juist, volledig en actueel zijn.
- **Vertrouwelijkheid:** de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.
- **Controleerbaarheid:** de mate waarin het mogelijk is om achteraf parameters die van belang zijn voor beschikbaarheid, integriteit of vertrouwelijkheid te verifiëren.

Onvoldoende informatieveiligheid kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de dagdagelijkse werking van de onderwijsinstelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoverlies.

1.2 TOELICHTING PRIVACY

Privacy gaat over de verwerking van persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform de huidige wet- en regelgeving. De bescherming van de privacy regelt onder andere de voorwaarden waaronder persoonsgegevens gebruikt mogen worden.

Persoonsgegevens zijn hierbij alle gegevens van een geïdentificeerd of identificeerbaar individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. Denken we maar aan het verzamelen, raadplegen, bijwerken, verspreiden tot met het wissen van deze gegevens.

1.3 VERVLECHTING INFORMATIEVEILIGHEID EN PRIVACY

Informatieveiligheid is noodzakelijk om privacy te waarborgen. Beide begrippen zijn met elkaar verbonden. Het onderwerp informatieveiligheid en privacy wordt afgekort tot IVP. Deze beleidstekst ligt ten grondslag aan de aanpak van informatieveiligheid en privacy binnen SmdB De Springplank.

2 DOEL EN REIKWIJDTE

2.1 DOEL

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van het onderwijs en de dagdagelijkse werking van SmdB De Springplank.
- Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten zoveel mogelijk worden voorkomen.

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

2.2 REIKWIJDTE

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen SmdB De Springplank waaronder in ieder geval: alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties, evenals op andere betrokkenen waarvan SmdB De Springplank persoonsgegevens verwerkt.
- Dit beleid is van toepassing op de digitale en geschreven verwerking van persoonsgegevens.
- Het IVP-beleid geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties die uit hoofde van hun taak, op school of thuis persoonsgegevens verwerken.
- Het beleid heeft betrekking op gecontroleerde informatie die door onszelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en sociale media.
- Het IVP-beleid binnen SmdB De Springplank heeft raakvlakken met:
    - Algemeen veiligheids- en toegangsbeveiligingsbeleid; waaronder hulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen;
    - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties;
    - IT-beleid; met als aandachtspunten de aanschaf, het beheer, het gebruik en/of het uit dienst stellen van hardware, software, services en (digitale) leermiddelen;
    - Participatie van leerlingen, hun ouders/verzorgers en medewerkers.

3 UITGANGSPUNTEN

3.1 ALGEMENE BELEIDSUITGANGSPUNTEN

De belangrijkste beleidsuitgangspunten bij SmdB De Springplank zijn:

- IVP dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de **Algemene Verordening Gegevensbescherming** (AVG).
- De verwerking van persoonsgegevens is steeds gebaseerd op één van de in deze verordening vastgelegde rechtmatigheden. Hierbij willen we een goede balans zoeken tussen het belang van SmdB De Springplank om persoonsgegevens te verwerken en het belang van de betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn/haar persoonsgegevens.
- Het schoolbestuur, vzw SmdB De Springplank, is als rechtspersoon de **verwerkingsverantwoordelijke** voor alle persoonsgegevens die in opdracht van SmdB De Springplank verwerkt worden.
- SmdB De Springplank beheert ook informatie waarvan de intellectuele eigendom (het **auteursrecht**) toebehoort aan derden. Medewerkers en leerlingen moeten dus goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt daarom bij SmdB De Springplank geclassificeerd. Deze **classificatie** vormt het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik gemaakt wordt van de classificatie. Het beleid maakt een balans tussen de risico's van hetgeen we willen beschermen en de benodigde maatregelen.
- SmdB De Springplank sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) **verwerkersovereenkomsten** af indien deze persoonsgegevens ontvangen van de school.
- Binnen SmdB De Springplank is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van **iedereen**. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten.
- 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. In het *huishoudelijk reglement van het personeel van het vrij Protestants-Christelijk Onderwijs* (artikel 5 § 2/3, artikel 7 § 1/2, artikel 9 § 1/2) wordt hiernaar verwezen.
- Bij wijzigingen in de infrastructuur, de aanschaf en de uit dienst name van (informatie)systemen, wordt bij SmdB De Springplank steeds rekening gehouden met IVP.
- IVP is bij SmdB De Springplank een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

3.2 UITGANGSPUNTEN PRIVACY

De zes vuistregels rond de omgang van persoonsgegevens bij SmdB De Springplank 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 verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2 **Grondslag**: verwerking van persoonsgegevens is gebaseerd op één van de wettelijke rechtmatigheden: toestemming, overeenkomst, wettelijke verplichting, openbaar belang, 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 tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt.
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 IVP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op inzage, verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5 **Opslagbeperking:** data wordt niet langer bewaard dan noodzakelijk. De verwerking wordt door het IVP-beleid beperkt in de tijd.
6 **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn, en dat zij voldoende beschikbaar zijn om de werking van SmdB De Springplank te waarborgen. Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van **toestemming**, zal SmdB De Springplank een eenduidige procedure hanteren die een actieve en aantoonbare handeling vereist.

4 WET- EN REGELGEVING

SmdB De Springplank voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Algemene Verordening Gegevensbescherming (AVG)
- Camerawet
- Auteurswet

5 ORGANISATIE

De organisatie van IVP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Dit hoofdstuk beschrijft hoe IVP in SmdB De Springplank is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau wordt beschreven welke verantwoordelijkheden en taken de verschillende rollen met zich meebrengen.

5.1 ROLLEN (FUNCTIES) RONDOM IVP

Om IVP gestructureerd en gecoördineerd aan te pakken worden bij SmdB De Springplank een aantal rollen aan medewerkers in de bestaande organisatie toegewezen.

5.2 RICHTINGGEVEND

Verwerkingsverantwoordelijke

Het schoolbestuur is eindverantwoordelijk voor IVP en stelt het beleid en de basismaatregelen op het gebied van IVP vast.

De toepassing en werking van het IVP-beleid wordt op basis van regelmatige rapportages geëvalueerd.

Zie bijlage 1 voor een schematische weergave van de rol- en taakverdelingen aangaande IVP op SmdB De Springplank en binnen vzw SmdB De Springplank.

5.3 STUREND

Data Protection Officer (DPO) van de koepelorganisatie (privacy@ipco.be)

Vanuit de koepelorganisatie Katholiek Onderwijs Vlaanderen wordt er een Data Protection Officer aangesteld. Deze zal binnen het schoolbestuur of instelling het Aanspreekpunt Informatieveiligheid (AIV) aansturen. De taak bestaat uit:

- schoolbesturen informeren en adviseren over hun verplichtingen vanuit de AVG en vanuit andere gegevensbeschermingsbepalingen;
- AIV's opleiden en hulpmiddelen verstrekken zodanig dat ze binnen hun instelling(en) het IVP-beleid kunnen ondersteunen;
- desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling;
- met de toezichthoudende autoriteit samenwerken en optreden als aanspreekpunt voor deze autoriteit.

Aanspreekpunt Informatieveiligheid (aiv.despringplank@gmail.com)

Het AIV is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (directie van de instelling, raad van bestuur van het schoolbestuur) en staat de mensen op uitvoerend niveau bij. Het AIV moet:

- ervoor zorgen dat het beleid vertaald wordt naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen SmdB De Springplank
- Meewerken aan en aansturen op de bewustmaking en opleiding van het personeel
- Het aanspreekpunt zijn voor incidenten op het gebied van IVP
- De verdere afhandeling van incidenten binnen SmdB De Springplank coördineren

5.4 UITVOEREND

Leidinggevende

Naleving van het Informatieveiligheidsbeleid 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 IVP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IVP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IVP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door het AIV.

Ict-coördinator

De ict-coördinator vormt een technisch aanspreekpunt inzake informatieveiligheid voor het management en de medewerkers, en zorgt in de praktijk voor de implementatie van toegangsrechten en de rapportage aangaande digitale informatieveiligheid.

Medewerker

Alle medewerkers hebben een verantwoordelijkheid met betrekking tot informatieveiligheid in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het privacyreglement en eraan toegevoegde nota's en visieteksten aangaande IVP op SmdB De Springplank. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists, formulieren en praktische tools.

Medewerkers wordt gevraagd om actief betrokken te zijn bij informatieveiligheid. Dit kan door meldingen te maken van veiligheidsincidenten, het doen van voorstellen ter verbetering van IVP en het uitoefenen van invloed op het beleid (individueel of via de ervoor voorziene overlegorganen en/of via het aanspreekpunt). Zelf hebben zij ook een voorbeeldfunctie naar andere medewerkers, externen en vooral leerlingen toe.

Van ambtswege uit, of eventueel contractueel, worden alle medewerkers (ook extern) van SmdB De Springplank die toegang kunnen hebben tot persoonsgegevens, gebonden aan een discretieplicht. Welbepaalde (externe) medewerkers zijn wettelijk gebonden aan een beroepsgeheim.

6 CONTROLE EN RAPPORTAGE

Dit IVP-beleid en alle bijhorende richtlijnen, nota's en tools, worden minimaal elke twee jaar getoetst en bijgesteld door het schoolbestuur. Hierbij wordt rekening gehouden met:

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

Daarnaast kent SmdB De Springplank een jaarlijkse planning en controlecyclus voor IVP. Dit is een vast evaluatieproces waarmee de inhoud en effectiviteit van het IVP-beleid 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, alsmede over doelen, bereik en ambitie op het gebied van IVP.
- **tactisch** niveau (sturend) de strategie wordt vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **operationeel** niveau (uitvoerend) de onderwerpen worden besproken die de dagelijkse uitvoering aangaan. Deze overlegvorm wordt niet centraal georganiseerd, en indien nodig in elk organisatieonderdeel van SmdB De Springplank afzonderlijk.

6.1 VOORLICHTING EN BEWUSTZIJN

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatieveiligheid en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij SmdB De Springplank 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 onder andere de regelmatig terugkerende bewustwordingscampagnes voor iedereen binnen de school. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van het AIV en leidinggevende(n), met de raad van bestuur van vzw SmdB De Springplank als eindverantwoordelijke.

6.2 CLASSIFICATIE EN RISICOANALYSE

Bij SmdB De Springplank heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. De risicoanalyse zal het niveau van de beveiligingsmaatregelen bepalen rekening houdend met de classificatie van de gegevens. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang zijn voor de informatievoorziening.

6.3 INCIDENTEN EN DATALEKKEN

Bij SmdB De Springplank is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Alle incidenten kunnen worden gemeld bij aiv.despringplank@gmail.com. De afhandeling van deze incidenten volgt een gestructureerd proces, waarbij men ook voorziet in de juiste stappen rondom de meldplicht datalekken.

6.4 CONTROLE, NALEVING EN SANCTIES

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IVP proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij SmdB De Springplank wordt actief aandacht besteed aan IVP bij de aanstelling, tijdens functioneringsgesprekken, met een gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Mocht de naleving ernstig tekort schieten, dan kan SmdB De Springplank de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden. Voor de bevordering van de naleving van de AVG heeft het AIV een belangrijke rol.

7 BIJLAGE 1: TABEL IVP ROLLEN EN TAKEN

Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
School- of centrumbestuur	• Eindverantwoordelijke • IVP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IVP-beleid op basis van rapportages en bijsturen van dit beleid indien nodig • Organisatie IVP inrichten	• Informatieveiligheids- en privacy beleid opstellen en goedkeuren en communiceren • Aanspreekpunt informatieveiligheid aanstellen • Oprichten veiligheidscel
Leidinggevende (directie)	• Toezien op de naleving van het IVP-beleid en privacywetgeving en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Communicatie naar alle betrokkenen; er voor zorgen dat alle medewerkers op de hoogte zijn van het IVP-beleid en de consequenties ervan. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IVP-beleid. • Rapporteren voortgang m.b.t. doelstellingen IVP-beleid aan bestuur • Periodiek het onderwerp informatiebeveiliging onder de aandacht brengen in werkoverleg, beoordelingen,… • Implementeren IVP-maatregelen.	Communiceren, informeren en toezien op naleving van o.a.: • IVP in het algemeen • Hoe omgaan met leerlingendossiers • Wie mag wat zien • Gedragscode • Beveiliging van ruimtes • Preventieve maatregelen (o.a. brand en waterschade aan servers…) • …
Data protection officer koepel	• Schoolbesturen informeren en adviseren over hun verplichtingen krachtens de AVG en regelgeving. • Richtlijnen, kaders, procedures opstellen en aanbevelingen doen m.b.t. informatieveiligheid en privacy • Aanspreekpunten IVP opleiden en hen de nodige tools en hulpmiddelen verstrekken. • Desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling. • Samenwerken met de toezichthoudende autoriteit en optreden als aanspreekpunt voor deze autoriteit. • Brugfiguur naar de externe partijen toe. • Lerend netwerk ontwikkelen en aansturen.	• Opstellen van algemene processen, richtlijnen en sjablonen IVP • Nascholingstraject organiseren • Overleg met informatieveiligheidsconsulenten onderwijsnetten en GO! • Overleg met externe partijen: leveranciers van leerlingadministratie en -volgsysytemen en leveranciers van didactische software • Tools aanpassen/ontwikkelen

Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**

Aanspreekpunt informatieveiligheid	• Informeert en adviseert directie/bestuur en personeel over IVP
	• Rapporteert naar directie/bestuur
	• Informeert de data protection officer van de koepel
	• Meewerken aan de uitwerking van een specifiek IVP-beleid op basis van het algemeen IVP-beleid
	• Voorstellen doen tot aanpassingen van centraal aangeboden processen, richtlijnen en procedures om de uitvoering van het IVP-beleid te ondersteunen binnen de school
	• Meewerken aan:
	  ○ classificatie van middelen
	  ○ risicoanalyse
	  ○ het opstellen van een veiligheidsplan
	• Aanspreekpunt voor IVP-incidenten
	• Incidentafhandeling (registreren en evalueren).
	• Invullen register verwerkingsactiviteiten
		Voorstellen van aanpassingen aan de uitgewerkte formulieren van processen, richtlijnen en procedures rond IVP, bijvoorbeeld:
		
		• Security awareness activiteiten
		• Authenticatie en autorisatie-beleid
		• Gedragscodes (ICT en internetgebruik, sociale media, privacybeleid…) naar medewerkers en leerlingen toe
		• Verwerkersovereenkomsten regelen
		• Toestemming opstellen gebruik foto's en video
		• Communicatieplan naar medewerkers, leerlingen, ouders en cursisten
		• Procedure IVP-incident afhandeling
		• Inrichten meldpunt datalekken
		• Melden datalekken naar de overheid toe
		• …
		Invullen van register verwerkingsactiviteiten voor schooleigen situatie

Informatieveiligheids cel (CIV) van de school of het schoolbestuur [1]	• Classificatie van informatie • IVP risicoanalyse uitvoeren • Prioriteiten voorstellen • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten bekrachtigen door bestuur • De toegangsrechten van gebruikers regelmatig beoordelen en controleren. • Evalueren IVP-beleid en voorstellen van verbetermaatregelen • Bespreking veiligheidsincidenten en voorstellen formuleren voor te nemen maatregelen • Aanpassen gegevensbeschermings-effectbeoordeling aan eigen situatie	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) • Classificatie van informatiebronnen en persoonsgegevens • Risicoanalyse uitvoeren en documenteren Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
Iedereen	• Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IVP bij de dagelijkse werkzaamheden	Richtlijnen en procedures volgen Melden incidenten aan aanspreekpunt informatieveiligheid

[1] bestaande uit aanspreekpunt informatieveiligheid, coördinerend directeur SG, algemeen secretaris. Directie vertegenwoordiging in overlegorgaan DB (dagelijks bestuur)

8 BIJLAGE 2: AANVULLENDE NOTA'S

Bij dit algemene deel van het IVP-beleid horen nog enkele specifieke nota's :

- Classificatie van persoonsgegevens
- Toegangsmatrices
- Wachtwoordbeleid
- Communicatiebeleid
- Toestelbeleid
- Backupbeleid

Tevens is er een bijkomend document voorzien, met de nodige achtergrondinformatie bij deze nota.

CLASSIFICATIE VAN PERSOONSGEGEVENS

vzw SmdB De Springplank

voor:

SmdB De Springplank

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB).

Onderwerp	Implementatie - termijn				Implementatie - praktisch	
	OK	25/05/2018	01/09/2018	01/09/2019	Intern	AIV
BIV-Classificatie persoonsgegevens		X				X

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-03-05	werkdoc	Jasper Vanwalleghem	Markering: invullen school/ instelling/ bestuur adhv 'zoek & vervang' Markering: te bespreken
1.1	2018-03-06	werkdoc	Jasper Vanwalleghem	Toepassen lay-out huisstijl IPCO
1.2	2018-04-24	werkdoc	Jasper Vanwalleghem	Aanpassen vorm categorieën persoonsgegevens conform Register, inhoud blijft gelijk (markering groen)
1.3	2018-05-15	werkdoc	Jasper Vanwalleghem	Uniformiseren verwijzingen #...#
1.4	2018-07-01	Werkdoc	Jonathan De Laet Karolien Deraeve	Markeringen invullen + overleg
1.5	2018-08-25	Publiek	Jonathan De Laet	Finaliseren voor publicatie

1 INLEIDING

1.1 SITUERING

Door een classificatie van persoonsgegevens te maken, kan men op SmdB De Springplank op een gestructureerde manier de beveiliging van deze gegevens vorm geven. De classificatie gebeurt op basis van drie aspecten:

- beschikbaarheid;
- integriteit;
- vertrouwelijkheid.

Men spreekt ook wel eens van een BIV-classificatie. Voor elk aspect wordt in dit beleid een classificatie in niveaus gehanteerd, bv. **laag – midden – hoog**.

Op basis van de in deze nota uitgewerkte classificatie, bepaalt men op SmdB De Springplank de nodige organisatorische en technische maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid gepast te waarborgen.

Deze nota valt onder de eindverantwoordelijkheid van vzw SmdB De Springplank.

1.2 HOE WORDT HET CLASSIFICATIENIVEAU BEPAALD?

Dit doen we op SmdB De Springplank door gebruik te maken van de vragen, zoals deze zijn opgesteld voor het respectievelijke schema (zie onderstaande). Het is hierbij in zekere zin belangrijker om met een aantal mensen te praten over deze vragen, dan een exacte inschatting te maken. Door erover te praten kweek je bewustwording en ga je anders naar de processen kijken.

1.3 WELKE PERSOONSGEGEVENS WORDEN ER VERWERKT?

Samengevat verwerkt SmdB De Springplank de onderstaande categorieën van persoonsgegevens.

1.3.1 LEERLINGENADMINISTRATIE

- **Identificatiegegevens:** naam en adresgegevens van leerlingen en ouders, telefoon, noodtelefoon, mailadres, klas, stamboeknummer,
- **Financiële bijzonderheden:** rekeningnummer ouders (indien domiciliëring), openstaand saldo schoolrekening, betaalplan
- **Persoonlijke kenmerken:** geslacht, geboortedatum, geboorteplaats, nationaliteit, burgerlijke staat ouders, hoederecht, vonnis
- **Leefgewoonten:** registratie afwezigheden, verplaatsing thuis-school
- **Samenstelling van het gezin**
- **Opleiding en vorming:** instellingen, jaren, klassen (leerling)
- **Rijksregisternummer**

- **Moeder bezit diploma secundair onderwijs**
- **School:** aanwezigheden oudercontact (ouders)
- **Filosofische of religieuze overtuiging:** in het kader van het beleven van de feestdagen inherent aan de door de grondwet erkende levensbeschouwelijke overtuiging van de leerling
- **Beeldopnamen:** pasfoto (ter identificatie van de leerling)

1.3.2 LEERLINGENBEGELEIDING

- **Identificatiegegevens:** naam en adresgegevens van leerlingen en ouders, telefoon, noodtelefoon, mailadres, klas, stamboeknummer
- **Persoonlijke kenmerken:** geslacht, geboortedatum, geboorteplaats, nationaliteit, burgerlijke staat ouders, hoederecht, vonnis
- **Functioneren:** gedrag, welbevinden, communicatie met leerkrachten & medeleerlingen, groepsdynamiek (sociogram), handelingsplannen, begeleiding, opvolging, straffen, sancties, tucht
- **Evaluatie:** puntenboeken, observaties, evaluaties, remediëring, rapporten, commentaren, deliberaties, verslagen, eindbeslissingen, motiveringen
- **Vrijetijdsbesteding en interesse:** talenten, interesses
- **Gegevens betreffende de gezondheid:** lichamelijke, psychische gezondheidsgegevens & risicosituaties (conform de wetgeving, met oog op begeleiding), ook zorgdiagnoses, -dossiers en medische begeleiding (intern en extern)

1.3.3 PERSONEELSADMINISTRATIE

- **Identificatiegegevens:** naam en adresgegevens, identiteitskaartnummer, nummer vaste en mobiele telefoon, mailadres, stamboeknummer
- **Financiële bijzonderheden:** bankrekeningnummer, onkostenvergoedingen
- **Persoonlijke kenmerken:** geslacht, geboortedatum, geboorteplaats, burgerlijke staat, nationaliteit
- **Leefgewoonten:** registratie afwezigheden, bewijzen
- **Samenstelling van het gezin**
- **Opleiding en vorming:** diploma's, bekwaamheidsbewijzen
- **Beroep en betrekking:** opdrachten, verlofstelsels, anciënniteit
- **Rijksregisternummer**
- **Gegevens betreffende de gezondheid:** attest medische geschiktheid
- **Beeldopnamen:** pasfoto

1.3.4 PERSONEELSBEHEER

- **Identificatiegegevens:** naam en adresgegevens, identiteitskaartnummer, nummer vaste en mobiele telefoon, mailadres, stamboeknummer
- **Persoonlijke kenmerken:** geslacht, geboortedatum, geboorteplaats, burgerlijke staat, nationaliteit
- **Leefgewoonten:** registratie afwezigheden, bewijzen
- **Gegevens betreffende de gezondheid:** attest medische geschiktheid
- **Opleiding en vorming:** diploma's, bekwaamheidsbewijzen, nascholingen
- **Loopbaanbegeleiding:** curriculum vitae, sollicitatie, functionerings- & evaluatiegesprekken
- **Levensbeschouwing:** indien (gedeeltelijk) leerkracht Godsdienst

1.3.5 COMMUNICATIE

- **Beeldopnamen:** enkel mits toestemming, ter communicatie via schoolwebsite, (nieuws)brief, Facebook

1.3.6 TOEZICHT TELECOMACTIVITEITEN

- **Identificatiegegevens:** d.m.v. logging (cf. toestelbeleid)

2 BESCHIKBAARHEID

2.1 OMSCHRIJVING

Hiermee bedoelen we de mate waarin de gegevens en diensten beschikbaar zijn, zodanig dat het onderwijsgebeuren ongestoord voort kan gaan.

Deelaspecten hiervan zijn:

- **Continuïteit:** de mate waarin de beschikbaarheid gewaarborgd is;
- **Portabiliteit:** de mate waarin de overdraagbaarheid van informatie naar andere gelijksoortige technische infrastructuren gewaarborgd is;
- **Herstelbaarheid:** de mate waarin de informatie of dienst tijdig en volledig hersteld kan worden in geval van onderbrekingen, pannes, onderhoud, ...

Voor de beschikbaarheid komt de classificatie respectievelijk overeen met: ***niet nodig, onbelangrijk, belangrijk, essentieel***.

Niveau 1: Beschikbaarheid is niet nodig	**Niveau 2:** Beschikbaarheid is onbelangrijk	**Niveau 3:** Beschikbaarheid is belangrijk	**Niveau 4:** Beschikbaarheid is noodzakelijk
Het systeem of de informatie is niet (meer) nodig voor de werking van de instelling.	*Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meerdere dagen brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.*	*Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.*	*Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.*
Overeenkomstige score van het beschikbaarheidsschema (zie verder)			
Tussen 0 en 2	Tussen 3 en 7	Tussen 8 en 12	Tussen 13 en 15

2.2 BESCHIKBAARHEIDSSCHEMA

Dit schema kan per toepassing ingevuld worden.

Plaats een 'x' in de bijhorende kolom om de classificatie te maken, en motiveer elke vraag. Tel het eindtotaal op om de classificatie van de toepassing te bekomen (zie tabel in § 2.1). Nul is "n.v.t."

Vragen	0	1	2	3	Motivatie
Wat is de verwachte belasting van de toepassing? *1 = weinig gelijktijdige gebruikers, weinig transacties* *2 = veel gelijktijdige gebruikers, normale hoeveelheid transacties* *3 = veel gelijktijdige gebruikers, veel transacties*					
Zijn er contractuele of wettelijke verplichtingen voor de beschikbaarheid? *1 = nee, of regulier* *2 = ruime of hoge contractuele verplichtingen* *3 = wettelijke verplichtingen, desgevallend enkel voor bepaalde periodes in het schooljaar*					
Wat is de maximale periode dat de toepassing niet- beschikbaar mag zijn (in de loop van het schooljaar)? *1 = maximaal enkele dagen of een week* *2 = maximaal een werkdag* *3 = maximaal een aantal uur*					
Hoe erg is het als de gegevens en/of de toepassing niet beschikbaar zijn? *1 = niet cruciaal voor de kerntaken* *2 = het lesgeven ondervindt hinder, maar kan doorgaan* *3 = het lesgeven (of cruciale deelaspecten ervan) kunnen niet doorgaan*					
Leidt het niet beschikbaar zijn van de toepassing tot imagoverlies? *1 = nee* *2 = kortstondig maar kan opgevangen of hersteld worden met goede communicatie* *3 = langdurig of blijvend imagoverlies*					

3 INTEGRITEIT

3.1 OMSCHRIJVING

Hiermee wordt bedoeld of de gegevens correct en actueel zijn. Deelaspecten hiervan zijn:

- **Juistheid**: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
- **Volledigheid**: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
- **Waarborging**: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Voor de integriteit komt de classificatie respectievelijk overeen met: ***niet noodzakelijk, noodzakelijk, vereist, absoluut***.

Niveau 1: Integriteit is niet noodzakelijk.	**Niveau 2:** Integriteit is noodzakelijk.	**Niveau 3:** Integriteit is vereist.	**Niveau 4:** Integriteit is absoluut.
Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn. Indien informatie niet correct is, leidt dit tot beperkte schade.	*Blijvende juistheid van informatie moet maximaal gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is, kan de organisatie substantiële schade lijden.*	*Informatie moet gegarandeerd correct zijn. Het is echter niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is, kan de organisatie ernstige schade lijden.*	*Informatie moet gegarandeerd correct zijn. Informatie waarbij het noodzakelijk is dat de correctheid niet betwist kan worden, zoals de uitslagen van toetsen, examens, onomkeerbare financiële transacties. Indien informatie niet correct is, kan de organisatie ernstige schade lijden.*
Overeenkomstige score in het Integriteitsschema (zie verder)			
Tussen 0 en 2	Tussen 3 en 7	Tussen 8 en 13	Tussen 14 en 18

3.2 INTEGRITEITSSCHEMA

Dit schema kan per toepassing ingevuld worden.

Plaats een 'x' in de bijhorende kolom om de classificatie te maken, en motiveer elke vraag. Tel het eindtotaal op om de classificatie van de toepassing te bekomen (zie tabel in § 3.1). Nul is "n.v.t."

Vragen	0	1	2	3	Motivatie
Kan er fraude met leerresultaten of financiële fraude plaatsvinden door fouten in de gegevens of ongeautoriseerde wijzigingen? *1 = nee, de gegevens lenen zich bijna niet voor fraude* *2 = beperkt, gegevens worden ook elders gecontroleerd* *3 = ja, de toepassing is de enige met deze gegevens*					
Hoe erg is het als er fouten of ongeautoriseerde veranderingen in de gegevens zitten? *1 = niet* *2 = het lesgeven wordt belemmerd maar kan wel doorgaan* *3 = het lesgeven kan niet doorgaan, of er is permanent nadeel*					
Hoeveel effect hebben fouten of ongeautoriseerde veranderingen in gegevens? *1 = alleen intern* *2 = intern en mogelijk is een andere partij beïnvloed* *3 = in een hele keten*					
Leiden fouten of ongeautoriseerde veranderingen tot imagoverlies? *1 = nee* *2 = kortstondig imagoverlies* *3 = langdurig imagoverlies*					
Zijn er contractuele of wettelijke verplichtingen voor de integriteit van gegevens? *1 = nee* *2 = ja, deze eisen stelselmatige controle* *3 = ja, deze eisen stelselmatige controle en bewijs van werking (= rapportering)*					
Kunnen er personen negatieve gevolgen ondervinden als gevolg van het niet correct zijn van gegevens? *1 = niet* *2 = eventuele fouten zijn nog te verbe-teren* *3 = fouten veroorzaken ernstige of langdurige negatieve gevolgen*					

4 VERTROUWELIJKHEID

4.1 OMSCHRIJVING

Hiermee wordt de mate bedoeld, dat de juiste personen en systemen toegang krijgen tot de gegevens in kwestie.

Deelaspecten hiervan zijn:

- **Authenticatie:** *is het proces waarbij je je identiteit gaat bewijzen (ben je wel diegene die je beweert te zijn). Vaak doen we dit door combinatie van een gebruikersnaam en een wachtwoord.*
- **Autorisatie:** *is een proces waarbij onderzocht wordt of je voldoende rechten hebt of toestemming hebt voor hetgeen je wilt doen. Bijvoorbeeld: een leerkracht zal toestemming hebben om in het puntenboek van de klas te schrijven, de leerling mag alleen zijn eigen punten lezen. Enkel de zorgverantwoordelijke en de directie kan in het zorgdossier van een leerling schrijven.*
- **Auditing (Controleerbaarheid):** *is het proces waarmee je kan nagaan wie wat waar, wanneer en waarmee doet. Vaak heb je hiervoor een hulpmiddel nodig dat je kan vertellen wat er op elk moment gebeurde. Dit kan onder meer in de vorm van een logboek.*

Voor de vertrouwelijkheid komt de classificatie respectievelijk overeen met: ***openbaar, intern, vertrouwelijk, geheim***.

Niveau 1: Informatie is openbaar	**Niveau 2:** Informatie is intern	**Niveau 3:** Informatie is vertrouwelijk.	**Niveau 4:** Informatie is geheim.
Openbaar worden van gegevens leidt tot weinig of geen schade voor een instelling of betrokkene.	*De organisatie, instelling of betrokkene kan niet meteen substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen, maar informatie mag wel alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know)*	*De organisatie, instelling of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know)*	*De organisatie, instelling of betrokkene kan ernstige schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer geselecteerde groep personen. Hieronder vallen onder andere bijzondere persoonsgegevens.*

4.2 VERTROUWELIJKHEIDSSCHEMA

Hieronder staat de classificatie van categorieën van persoonsgegevens, zoals ze op SmdB De Springplank gehanteerd wordt.

Categorie van persoonsggevens	Openbaar	Intern	Vertrouwelijk	Geheim	Motivatie
Leerlingenadministratie					
Rijksregisternummer			x		*De instelling is gemachtigd om het rijksregisternummer te verwerken, maar mag het niet extern ter beschikking stellen.*
Identificatiegegevens			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Persoonlijke kenmerken			x		*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Leefgewoonten			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Samenstelling van het gezin			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Opleiding en vorming			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
School			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Filosofische of religieuze overtuiging			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Beeldopnamen: pasfoto		x			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*

Categorie van persoonsgegevens	Openbaar	Intern	Vertrouwelijk	Geheim	Motivatie
Leerlingenbegeleiding					
Functioneren			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Evaluatie			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Vrijetijdsbesteding en interesse			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Gegevens betreffende de gezondheid				x	*De instelling heeft deze gevoelige informatie nodig, maar dient deze zorgvuldig af te schermen.*

Categorie van persoonsgegevens	Openbaar	Intern	Vertrouwelijk	Geheim	Motivatie
Personeelsbeheer					
Identificatiegegevens			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Opleiding en vorming		x			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Loopbaanbegeleiding				x	*De instelling heeft deze gevoelige informatie nodig, maar dient deze zorgvuldig af te schermen.*
Levensbeschouwing				x	*De instelling heeft deze gevoelige informatie nodig, maar dient deze zorgvuldig af te schermen.*

Categorie van persoonsgegevens	Openbaar	Intern	Vertrouwelijk	Geheim	Motivatie
Personeelsadministratie					
Identificatiegegevens			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Persoonlijke kenmerken		x			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Financiële bijzonderheden			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Leefgewoonten			x		*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Samenstelling van het gezin			x		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*
Opleiding en vorming		x			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Beroep en betrekking		x			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*
Rijksregisternummer			x		*De instelling is gemachtigd om het rijksregisternummer te verwerken, maar mag het niet extern ter beschikking stellen.*
Gegevens betreffende de gezondheid				x	*De instelling heeft deze gevoelige informatie nodig, maar dient deze zorgvuldig af te schermen.*
Beeldopnamen (pasfoto)		x			*De instelling heeft deze informatie nodig, maar mag het niet extern ter beschikking stellen.*

Categorie van persoonsgegevens	Openbaar	Intern	Vertrouwelijk	Geheim	Motivatie
Communicatie					
Beeldopnamen	X				***ENKEL MITS TOESTEMMING!***
Toezicht telecomactiviteiten					
Identificatiegegevens			X		*De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.*

TOEGANGSMATRICES

vzw SmdB De Springplank

voor:

SmdB De Springplank

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB).

Onderwerp	Implementatie - termijn				Implementatie - praktisch	
	OK	25/05/2018	01/09/2018	01/09/2019	Intern	AIV
Toegangsmatrices		X			X	

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-03-05	werkdoc	Jasper Vanwalleghem	Markering: invullen school/ instelling/ bestuur adhv 'zoek & vervang' Markering: te bespreken
1.1	2018-03-06	werkdoc	Jasper Vanwalleghem	Toepassen lay-out huisstijl IPCO
1.2	2018-05-07	werkdoc	Jasper Vanwalleghem	Toevoegen codi aan toegangsmatrix
1.3	2018-05-15	werkdoc	Jasper Vanwalleghem	Aanpassen vorm categorieën persoonsgegevens conform Register, inhoud blijft gelijk (markering groen)
	2018-05-15	werkdoc	Jasper Vanwalleghem	Uniformiseren wijzigingen #...#
1.4	2018-07-01	Werkdoc	Jonathan De Laet Karolien Deraeve	Markeringen invullen + overleg
1.5	2018-08-25	Publiek	Jonathan De Laet	Finaliseren voor publicatie

1 INLEIDING

1.1 SITUERING

In deze nota bepalen we het gebruikersrechtenbeleid op SmdB De Springplank, gebaseerd op de ***classificatie van (persoons)gegevens***. Hiermee bedoelen we dat hier omschreven wordt welke gebruikers(groepen) welke toegangen hebben tot bepaalde gegevens. Hiervoor worden de vertrouwelijkheidsniveaus gehanteerd.

Bepaalde (persoons)gegevens en systemen worden meer specifiek vastgelegd in deze nota, teneinde dit gebruikersrechtenbeleid voldoende gedetailleerd uit te werken.

Deze nota valt onder de eindverantwoordelijkheid van vzw SmdB De Springplank.

1.2 GEBRUIKERSGROEPEN

Alle dragers, platformen, systemen en het netwerk die binnen SmdB De Springplank gebruikt worden, vallen onder het IVP-beleid. Dit houdt in het bijzonder in dat elk van deze dragers, platformen, systemen en het netwerk voorzien zijn van **beveiligingsgroepen**, waartoe de respectievelijke gebruikers behoren na authenticatie. (Zie het ***toestelbeleid*** en ***wachtwoordbeleid***.)

De volgende gebruikersgroepen worden hierbij gehanteerd:

- *ICT-coördinatoren*
- *CLB-medewerkers*
- *Directieleden*
- *Zorgverantwoordelijken (ZoCo en zorgleerkracht?)*
- *Leerkrachten*
    - *Die les geven aan betrokken leerling*
    - *Die geen les geven aan betrokken leerling*
- *Secretariaat*
    - *Die bevoegd zijn om (in welbepaalde zin) gegevens van leerlingen te verwerken*
    - *Die bevoegd zijn om (in welbepaalde zin) personeelsgegevens te verwerken*
    - *Die bevoegd zijn om financiële gegevens te verwerken*
    - *Die hier niet voor bevoegd zijn*
- *Ouder(s) of voogd, stiefouder(s)*
- *Betrokkene zelf*

Derden (bv. onderhoudspersoneel, externe betrokkenen) [2]

Deze groepen worden globaal gehanteerd binnen het IVP-beleid van SmdB De Springplank. Mogelijks bestaan er, voor welbepaalde gevallen of toepassingen, hiernaast nog specifiekere beveiligingsgroepen.

[2] Hiertoe behoren bv. de medewerkers van externe verwerkers, die in opdracht van SmdB De Springplank persoonsgegevens ontvangen en/of verwerken.

1.3 GEBRUIKERSRECHTEN

De algemeen gehanteerde gebruikersrechten zijn:

- GT: geen toegang (*men kan de gegevens niet opvragen, ook niet in overzichten e.d. vermeld*);
- L: leestoegang (*men kan alles zien, maar niets verwijderen, toevoegen of aanpassen*);
- W: wijzig- of schrijftoegang (*men kan alles zien, items toevoegen en aanpassen*)[3];
- D: verwijdertoegang (*men kan alles zien, items toevoegen, aanpassen en verwijderen*);
- VB: volledig beheer (*dit wil zeggen dat men ook de toegangsrechten, van zichzelf en van anderen, kan aanpassen*).

2 TOEGANGSMATRICES

Voor de opsomming van de concrete gegevens die zich in de hier gehanteerde vertrouwelijkheids-niveaus bevinden: zie de ***classificatie van persoonsgegevens***. Indien een bepaalde gebruikersgroep niet tot de matrix behoort, hebben deze mensen sowieso geen toegang (GT). Dit noemt men het **privacy by default**-principe.

2.1 LEERLINGENADMINISTRATIE

<table>
<tr><th></th><th>ICT-coördinatoren</th><th>CLB-medewerkers</th><th>Directieleden, Bestuur</th><th>Zorgverantwoordelijken</th><th>Leerkrachten (les)</th><th>Leerkrachten (geen les)</th><th>Secretariaat (bevoegd)</th><th>Ouder(s), voogd</th><th>Betrokkene zelf</th><th>Derden, externen</th></tr>
<tr><td>Openbaar</td><td colspan="10">Niet van toepassing</td></tr>
<tr><td>Intern</td><td rowspan="3">VB</td><td rowspan="3">L</td><td rowspan="3">L</td><td rowspan="3">WD</td><td>WD</td><td>L</td><td>WD</td><td rowspan="3" colspan="2">GT</td><td rowspan="3">GT</td></tr>
<tr><td>Vertrouwelijk</td><td rowspan="2">GT</td><td>L</td></tr>
<tr><td>Geheim</td><td>GT</td><td>GT</td></tr>
</table>

Specifieke rechten; uitzonderingen:

Financiële gegevens	GT	GT	L	GT		WD	GT	GT

Noten; toelichting:

- *Financiële gegevens: openstaande rekeningen en afbetalingen hoeven enkel maar door een beperkt aantal bevoegde personen verwerkt te worden.*
- *Ouder(s), voogden en betrokkenen zelf: hebben recht op informatie, inzage en correctie. Dit wil niet zeggen dat ze automatisch toegang tot de administratieve systemen moeten krijgen.*

[3] Mogelijks enkel voor gegevens die door de zichzelf toegevoegd werden (eigenaarschap), niet noodzakelijk ook voor gegevens van anderen. Een versiebeheersysteem bewaart een historiek.

2.2 LEERLINGENBEGELEIDING

	ICT-coördinatoren	CLB-medewerkers	Directieleden, Bestuur	Zorgverantwoordelijken	Leerkrachten (les)	Leerkrachten (geen les)	Secretariaat (bevoegd)	Ouder(s), voogd	Betrokkene zelf	Derden, externen
Openbaar	*Niet van toepassing*									
Intern	VB	L	L	WD	WD	L	WD	GT		GT
Vertrouwelijk						GT	GT			
Geheim	*Niet van toepassing*									

Noten; toelichting:

- *Ouder(s), voogden en betrokkenen zelf: hebben recht op informatie, inzage en correctie. Dit wil niet zeggen dat ze toegang tot het leerlingvolg- of leerlingevaluatiesystemen krijgen.*

2.3 PERSONEELSADMINISTRATIE

	ICT-coördinatoren	CLB-medewerkers	Directieleden	Zorgverantwoordelijken	Leerkrachten (les)	Leerkrachten (geen les)	Secretariaat (bevoegd)	Ouder(s), voogd	Betrokkene zelf	Derden, externen	Bestuur, DirCo SG
Openbaar	VB	L					WD	L			L
Intern		GT	WD	GT				GT			
Vertrouwelijk											
Geheim											

Specifieke rechten; uitzonderingen:

Financiële gegevens	VB	GT	L	GT	WD	GT	L

Noten; toelichting:

- *Betrokkene zelf: heeft recht op informatie, inzage en correctie. Dit wil niet zeggen dat hij/zij automatisch toegang tot de administratieve systemen krijgt, buiten de openbare gegevens.*

2.4 PERSONEELSBEHEER

	ICT-coördinatoren	CLB-medewerkers	Directieleden	Zorgverantwoordelijken	~~Leerkrachten (les)~~	~~Leerkrachten (geen les)~~	Secretariaat (bevoegd)	Ouder(s), voogd	Betrokkene zelf	Derden, externen	DirCo SG
Openbaar	VB	L					WD	L			
Intern		GT	WD	GT				GT			
Vertrouwelijk											
Geheim											

Noten; toelichting:

- *Betrokkene zelf: heeft recht op informatie, inzage en correctie. Dit wil niet zeggen dat hij/zij automatisch toegang tot de administratieve systemen krijgt, buiten de openbare gegevens.*

WACHTWOORDBELEID

vzw SmdB De Springplank

voor:

SmdB De Springplank

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB).

Onderwerp	Implementatie - termijn					Implementatie - praktisch	
	OK	25/05/2018	01/09/2018	01/09/2019	Schrappen	Intern	AIV
Toegangsbeheer			X			X	
Wachtwoordbepalingen en afraders			X			X	
Wachtwoordbeheer				X		X	
Meldpunt datalekken	X		X				X
Gebruik wachtwoordmanager/kluis				X		X	
2-factor authenticatie				X	X		X

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-03-05	werkdoc	Jasper Vanwalleghem	Markering: invullen school/ instelling/ bestuur adhv 'zoek & vervang' Markering: te bespreken
1.1	2018-03-06	werkdoc	Jasper Vanwalleghem	Toepassen lay-out huisstijl IPCO
1.2	2018-05-15	werkdoc	Jasper Vanwalleghem	Uniformiseren wijzigingen #...#
1.3	2018-07-01	Werkdoc	Jonathan De Laet Karolien Deraeve	Markeringen invullen + overleg
1.4	2018-08-25	Publiek	Jonathan De Laet	Finaliseren voor publicatie

1 INLEIDING

Een goed beveiligingsbeleid is tegenwoordig noodzakelijk voor elke school. Steeds meer privacygevoelige gegevens worden (online) gedeeld en een zwak beveiligingsbeleid zorgt ervoor dat je de deur openzet voor duidelijke risico's. Een goed beveiligingsbeleid geeft gebruikers (leerkrachten, leerlingen, CLB-medewerkers…) toegang tot alle informatie die ze nodig hebben om hun taak naar behoren uit te oefenen maar ontzegt hen alle toegang tot informatie die ze niet nodig hebben.

Er zijn drie pijlers waarop een goed beveiligingsbeleid berust:

- ***Authenticatie*** is het proces waarbij je je identiteit gaat bewijzen (ben je wel diegene die je beweert te zijn). Vaak doen we dit door combinatie van een gebruikersnaam en een wachtwoord.
- ***Autorisatie*** is een proces waarbij onderzocht wordt of je voldoende rechten hebt of toestemming hebt voor hetgeen je wilt doen.
- ***Auditing* (*Controleerbaarheid*)** is het proces waarmee je kan nagaan wie wat waar, wanneer en waarmee doet. Vaak heb je hiervoor een hulpmiddel nodig dat je kan vertellen wat er op elk moment gebeurde. Dit kan onder meer in de vorm van een logboek.

In dit document zullen we ons beperken tot de authenticatie en in het bijzonder het gebruik van wachtwoorden en andere, bijkomende authenticatiemethodes op SmdB De Springplank.

Deze nota valt onder de eindverantwoordelijkheid van vzw SmdB De Springplank.

2 TOEGANGSBEHEER

De directeur van de school is verantwoordelijk voor het gebruikersbeheer van de organisatie. Gebruikersbeheer houdt het aanmaken van gebruikers, toekennen van rechten en stopzetten van rechten in. Dit betekent dat er in de school een inventaris moet opgezet worden die het overzicht houdt van alle rollen en rechten gekoppeld aan personeelsleden in de school. Het opzetten van een dergelijke procedure rond het toegangsbeheer is belangrijk om de controle te kunnen houden op alle gebruikers die er zijn in de organisatie. Dit is de eerste stap in het authenticatiebeleid.

3 AUTHENTISEREN

Er zijn verschillende manieren om je in systemen te authentiseren. De meest gebruikte vorm is de combinatie van een gebruikersnaam en een wachtwoord. Een ander voorbeeld is het gebruik van je bankkaart en je pincode waarmee je je aan een bankautomaat kan authentiseren. Maar ook een vingerafdruk of een irisscan kan gebruikt worden om te kijken of je wel diegene bent die je beweert te zijn.

Wachtwoorden zorgen er mee voor dat de toegang tot applicaties goed beveiligd is. Het is dus van belang om een sterk beleid op te zetten om het inlogproces en -procedures te beheren. Op SmdB De Springplank werken we er continu aan om leerkrachten en leerlingen het belang van sterke wachtwoorden bij te brengen.

Een wachtwoordbeleid heeft als doel enkele bepalingen op te leggen rond het correct gebruik van wachtwoorden om de toegang tot gevoelige data (waaronder privacy gevoelige persoonsgegevens) te beveiligen middels een wachtwoord.

Een sterk wachtwoord is moeilijker te achterhalen en dus veiliger dan een 'zwak' wachtwoord. De sterkte van een wachtwoord hangt af van de lengte, complexiteit en de onvoorspelbaarheid.

3.1 WACHTWOORDBEPALINGEN

- Hoe langer een wachtwoord hoe beter. Het wachtwoord moet minstens 10 karakters hebben. (*Tegenwoordig zijn 8 karakters heel snel te raden.*)
- Beter nog is om te werken met een wachtwoordzin (bijv: `IkGaSinds2015NaarDeSchool`)
- Mix letters en tekens door elkaar: gebruik volgende karakters in het wachtwoord:
  - Hoofdletters
  - Kleine letters
  - Cijfers
  - Niet-alfanumerieke karakters
  - ➔ Bijv. `P@dd€nsto€l579`
- Gebruik de hoofdletters en andere karakters best niet in het begin van het wachtwoord/wachtzin en wissel ze met elkaar af. Bijv. `p@dd€NSto€l579`
- Keer woorden om. Bijv. `l€otSN€dd@p579`
- Maak wachtwoorden/wachtzinnen die enkel betekenis hebben voor jou.
- Het wordt aangeraden minstens één keer per schooljaar je wachtwoord te wijzigen.
- Gebruik verschillende wachtwoorden voor verschillende applicaties; hergebruik niet!
- Gebruik van wachtwoordmanagers of wachtwoordkluis kan hierbij een hulpmiddel zijn. Zie verder (14.6) voor mogelijkheden en opties.

3.2 AFRADERS

- Gebruik geen voor de hand liggende namen, woorden of getallen.
- Bijv. `NaamVoornaamGeboortedatum` of `StraatnaamNr`
- Schrijf het wachtwoord niet op: niet op papier, niet elektronisch in jouw GSM of PC. Bewaar ze zeker niet op een Post-it aan de computer.
- Indien je toch liefst je wachtwoord opschrijft, bewaar het dan ver van de gebruiker en schrijf er niet bij voor welke applicatie het dient.
- Geef het wachtwoord niet door, op geen enkele wijze aan niemand (ook niet aan ICT).
- Verzend nooit een wachtwoord via email of een ander communicatiesysteem. (Niemand van SmdB De Springplank zal ooit je wachtwoord, om eender welke reden, op deze manier opvragen.)
- Zorg dat niemand op je vingers kijkt bij het ingeven van een wachtwoord.

- Er is soms de optie om een wachtwoord (even) te tonen, zodat je typfouten kan controleren. Zorg dat er niemand meekijkt op het moment dat je dit gebruikt.
- Besteed bijzondere aandacht aan een externe projectie indien dat aangesloten is, zoals bv. een beamer of (groot) tweede scherm.
- Gebruik geen woord uit het woordenboek.
- Herhaal niet te veel karakters of nummers (bijv. `11223344`).
- Gebruik geen te makkelijke wachtwoorden (bijv. `NaamAchternaamGeboortejaar`, `azertyuiop`).
- Bewaar je wachtwoord niet in de browser.
- Maak geen gebruik van de functie om ingelogd te blijven in een bepaalde applicatie.
- Gebruik andere wachtwoorden dan privé-wachtwoorden.

3.3 WACHTWOORDBEHEER

Laat de computer nooit onbeheerd achter maar vergrendel het scherm of log uit. Na 5 minuten inactiviteit vergrendelt de computer automatisch indien het gebruikte platform dit mogelijk maakt.

3.4 WAT DOEN BIJ VERMOEDEN VAN MISBRUIK?

Misbruik kan ontvreemding of onrechtmatig gebruik van een wachtwoord zijn.

- Verander het wachtwoord onmiddellijk
- Neem direct contact op met het meldpunt datalekken: aiv.despringplank@gmail.com

Deze personen gaan na of er sprake is van een misbruik en proberen zo nodig de schade te herstellen.

3.5 WAT DOEN ALS HET WACHTWOORD VERGETEN WERD

Indien het platform over deze mogelijkheid beschikt, kan je de “wachtwoord vergeten”-optie gebruiken. Meestal zorgt dit ervoor dat er een link gestuurd wordt naar een vooraf ingesteld “backup” emailadres, waarmee men een nieuw wachtwoord kan instellen (zonder het vorige te kennen). Anders neem je contact op met de ICT-verantwoordelijke. Zij zullen dit opvolgen.

3.6 GEBRUIK VAN WACHTWOORDMANAGERS OF -KLUIS

Indien je te veel wachtwoorden moet onthouden, kan je gebruik maken van een wachtwoordkluis. Wachtwoord-kluizen slaan al de wachtwoorden versleuteld op in een beveiligd bestand. Dit bestand wordt geopend met één sterk wachtwoord. Dit wil zeggen dat er maar één wachtwoord meer nodig is om alle wachtwoorden veilig te ontsluiten.

De volgende wachtwoordkluizen werden veilig bevonden voor onze school:

- KeePass (http://keepass.info/)
- LastPass (https://lastpass.com/nl/)
- Dashlane (https://www.dashlane.com/)
- 1Password (https://agilebits.com/onepassword)
- Passwordsafe (https://www.pwsafe.net/)

4 GEBRUIK VAN TWO-FACTOR AUTHENTICATIE

Indien je echt met veel privacygevoelige persoonsgegevens werkt, is vaak een combinatie van gebruikersnaam en wachtwoord niet voldoende veilig. De gebruikersnaam is meestal gekend en een wachtwoord kan eventueel gestolen of ontfutseld worden. Daarom bestaan er two-factor authenticatiemethodes.

Een voorbeeld: naast het gebruik van een gebruikersnaam en wachtwoord krijg je op je gsm een beveiligingscode doorgestuurd die je dan extra moet ingeven vooraleer je toegang krijgt. Naast het weten van de gebruikersnaam en wachtwoord is het dus ook nodig dat je iets in je bezit hebt, zoals bijvoorbeeld een telefoon waar men via sms een code doorgestuurd krijgt.

Deze systemen zijn veel veiliger en worden binnen SmdB De Springplank dan ook aangeraden voor iedereen die aan de meest privacygevoelige gegevens binnen de onderwijsinstelling kan. Concreet denken we hierbij aan iedereen die toegang heeft tot *geheime* gegevens (zie ***classificatie van gegevens*** en de ***toegangsmatrices***).

Wanneer een platform de mogelijkheid heeft om een dergelijk systeem te implementeren moet het na een inschatting van de praktische haalbaarheid en een testpersoon/-periode ingevoerd worden.

5 RISICO'S

Aan een slecht wachtwoordbeleid zijn risico's verbonden. Met dit beleid willen we onderstaande risico's verkleinen en/of uitschakelen.

- **Identiteitsdiefstal:** iemand die jouw wachtwoord achterhaalt, kan zich binnen de systemen in kwestie voordoen met jouw identiteit. Alle handelingen die men met jouw account stelt, worden via logging teruggebracht naar uzelf en niet naar diegene die met uw digitale identiteit aan de haal ging.
- **Phishing:** via phishing proberen oplichters achter persoonlijke gegevens/wachtwoorden te komen, meestal via e-mail of telefoon. Met deze informatie kunnen oplichters persoonlijke gegevens stelen en publiceren.
- Zie ***Achtergrondinformatie*** – § 1 voor meer informatie rond "phishing".
- **Hacking:** door zwakke wachtwoorden wordt het zeer eenvoudig om in te breken in de informatiesystemen. Eens binnen in het systeem kan er zeer veel schade berokkend en kunnen gegevens gestolen worden.

Rond deze risico's worden alle personeelsleden, maar zeker ook de leerlingen en ouders, binnen SmdB De Springplank actief en herhaaldelijk gesensibiliseerd.

O.a. via Safe on Web kan er veel praktisch materiaal gevonden worden rond dit beleid en rond de hier vermelde risico's: https://www.safeonweb.be/nl/home

COMMUNICATIEBELEID

vzw SmdB De Springplank

voor:

SmdB De Springplank

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB).

Onderwerp	Implementatie - termijn					Implementatie - praktisch	
	OK	25/05/2018	01/09/2018	01/09/2019	Schrappen	Intern	AIV
E-mailbeleid: algemene accounts			X			X	
E-mailbeleid: privé-accounts				X		X	
E-mailbeleid: schoolaccount				X		X	
Communicatie-apps			X			X	
Social Media-protocol			X			X	

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-03-05	werkdoc	Jasper Vanwalleghem	Markering: invullen school/ instelling/ bestuur adhv 'zoek & vervang' Markering: te bespreken
1.1	2018-03-06	werkdoc	Jasper Vanwalleghem	Toepassen lay-out huisstijl IPCO
1.2	2018-05-15	werkdoc	Jasper Vanwalleghem	Uniformiseren wijzigingen #...#
1.3	2018-07-01	Werkdoc	Jonathan De Laet Karolien Deraeve	Markeringen invullen + overleg
1.4	2018-08-25	Publiek	Jonathan De Laet	Finaliseren voor publicatie

1 INLEIDING

De manier waarop personeelsleden, en ook leerlingen en ouders, communiceren maakt ook een deel uit van het IVP-beleid. In dit document worden enkele principes vastgelegd inzake interne én externe communicatie, teneinde er samen voor te zorgen dat de privacy, de informatieveiligheid op en het imago van SmdB De Springplank op een gepast niveau wordt behouden.

Deze nota valt onder de eindverantwoordelijkheid van vzw SmdB De Springplank.

2 DISCRETIEPLICHT

Alle personeelsleden van SmdB De Springplank zijn gebonden aan een **discretieplicht**, ten aanzien van de persoonsgegevens van leerlingen, ouders of het gezin, en eventueel ten aanzien van elkaars persoonsgegevens. In het *huishoudelijk reglement van het personeel van het vrij Protestants-Christelijk Onderwijs* (art. 6 § 5, art. 20 § 8) wordt hiernaar verwezen.

Dit betekent concreet dat zij van ambtswege uit, geen persoonsinformatie mogen vermelden of publiceren, buiten de daarvoor voorziene kanalen binnen SmdB De Springplank. Onderling informatie delen mag natuurlijk, maar dan via de hieronder vastgelegde kanalen en procedures, en steeds indien het in het belang is van het kind, de kinderen of eventueel de collega in kwestie.

Personeelsleden worden dus van ambtswege uit geacht om de geldende beveiligings- en privacy-procedures en -afspraken te volgen, teneinde het **accidenteel** verspreiden van persoonsgegevens te vermijden. Indien men vermoedt dat, door toedoen van uzelf of van anderen, er mogelijks persoonsgegevens buiten de context van deze discretieplicht “geraakt” zijn, dan dient men het aanspreekpunt informatieveiligheid en/of het meldpunt datalekken hierover te contacteren.

Voor SmdB De Springplank is het meldpunt datalekken: ***aiv.despringplank@gmail.com***

3 EMAILBELEID

Op SmdB De Springplank maken we onderscheid tussen drie categorieën van emailaccounts:

- Algemene schoolemail (zoals o.a. *info@...*, *directie@...*, *leerkrachten@...*, …). Omdat we op onze school voorlopig nog geen netwerk/domein hebben maken wij voor een aantal zaken gebruik van algemene Gmail-adressen.
- Privé (eigen provider- of zelf aangemaakte Gmail-, Outlook-, Live-, Yahoo- … accounts)
- Persoonlijke school- of werkemail (meestal in de vorm *voornaam.naam@... of juf/meester.voornaam.despringplank@...*)

Voor elk van deze categorieën leggen we in deze paragraaf een aantal richtlijnen / afspraken vast inzake het doel, gebruik én de beveiliging van de accounts in kwestie.

Algemene opmerking: *Verzend nooit een wachtwoord, voor eender welk platform, via email of een ander communicatiesysteem. Niemand van SmdB De Springplank zal op deze manier ooit een wachtwoord opvragen.*

3.1 ALGEMENE ACCOUNTS

Het beheer hiervan is toegewezen aan één of meerdere medewerkers.

Deze adressen worden vrij verspreid en gepubliceerd.

Indien het adres verwijst naar een groep van personen, dan dient men het steeds in "blind carbon copy" (BCC) te plaatsen, bijvoorbeeld 2degraaddespringplank@gmail.com

Het is de bedoeling dat steeds en enkel de bevoegde personen toegang hebben tot een algemene account.

3.2 PRIVÉ ACCOUNTS

Deze accounts worden bij voorkeur gebruikt voor niet-school gerelateerde communicatie of handelingen.

Deze adressen worden niet verspreid of gepubliceerd. Ze worden enkel intern gebruikt door directie, administratie of op eigen initiatief.

Het gebruik van dergelijke accounts is niet verboden op SmdB De Springplank, zolang het de professionele bezigheden niet hindert en de informatieveiligheid niet in het gedrang komt.

Concreet:

- Het is niet toegestaan om berichten te verzenden met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud.
- Het is niet toegestaan om berichten te verzenden met een (seksueel) intimiderende inhoud.
- Het is niet toegestaan om berichten te verzenden die (kunnen) aanzetten tot haat en/of geweld.

Gebruik geen privé accounts voor communicatie met collega's aangaande instellingsgebonden zaken of voor de communicatie met leerlingen, oud-leerlingen, ouders of externen (zie § 3.3).

Let er op bij het gebruik van privé accounts, op toestellen of een netwerk waarop zich ook persoonsgegevens van SmdB De Springplank bevinden, dat bijlagen, hyperlinks, tools … die met de privé accounts gebruikt worden, niet leiden tot beveiligingsgevaren zoals virussen, ransomware, phishing[4] enz. Eigenaars van accounts waarmee dergelijke beveiligings-risico's gedetecteerd worden, zullen steeds hierop aangesproken worden met mogelijke maatregelen als gevolg.

[4] Meer informatie over "phishing" is te vinden in § 1 van de ***achtergrondinformatie***.

3.3 SCHOOLACCOUNTS (WERKADRESSEN)

Deze zijn telkens toegewezen aan één medewerker en zijn identificeerbaar voor die functie / medewerker.

Deze adressen kunnen verspreid en gepubliceerd worden.

Gebruik deze accounts voor communicatie met collega's aangaande instellingsgebonden zaken of voor de communicatie met leerlingen, oud-leerlingen, ouders of externen.

Wanneer algemene accounts of schoolaccounts gebruikt worden om mails door te sturen naar privé accounts dan is dit enkel toegelaten wanneer de privé account enkel en alleen voor de bevoegde persoon toegankelijk is. Bijvoorbeeld is het niet toegestaan om een privé account van een leerkracht te gebruiken waarbij de partner van de leerkracht ook toegang heeft tot deze account of wanneer de account thuis op een PC open staat en iedereen die er gebruik van maakt de inhoud van mails die hierop toekomen kan inkijken.

Natuurlijk gelden dezelfde afspraken voor deze accounts als voor privé accounts:

- Deze accounts worden aan de medewerker voor professioneel gebruik toegewezen of beschikbaar gesteld. Gebruik is dus verbonden met taken die voortvloeien uit de functie.
- Beperkt persoonlijk gebruik van deze accounts is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik oplevert:
    - berichten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud
    - berichten met een (seksueel) intimiderende inhoud.
    - berichten die (kunnen) aanzetten tot haat en/of geweld.

Bijkomende afspraken: verzend bij voorkeur **geen gevoelige persoonsgegevens** over leerlingen via deze accounts, of via eender welk ander berichtensysteem (zie ook § 4).

- Dit maakt het voor de verantwoordelijken onmogelijk om iedereens privacy en/of de informatieveiligheid als geheel te waarborgen. Mogelijks leidt dit er toe dat SmdB De Springplank niet alle rechten en vrijheden van de betrokkenen kan waarborgen.
- Gevoelige informatie: o.a. gezinssituatie, psychosociaal, medisch, zorg, financieel.
- Gebruik het beveiligde leerlingvolgsysteem om deze informatie met de juiste collega's en medewerkers te delen.
- Indien u via dit emailaccount gevoelige persoonsgegevens ontvangt, plaats deze dan zo snel mogelijk in het **beveiligde leerlingvolgsysteem** en verwijder daarna alle communicaties die deze gegevens bevatten of behandelden (ook uit uw "Prullenmand").
- Gebruik dit account niet op het internet, voor platformen die niet nodig zijn om uw taak voor SmdB De Springplank uit te voeren of voor platformen **die niet "informatieveilig" beschouwd worden** door het aanspreekpunt informatieveiligheid. Contacteer voor vragen hierrond *aiv.despringplank@gmail.com* of *privacy@ipco.be*
- Wanneer u met meerdere mensen moet communiceren gebruik dan BCC. Dat voorkomt dat gevoelige informatie door een "antwoord aan iedereen" bij onbevoegden terecht komt.
- Denk hierbij goed na aan wie u allemaal de gevoelige gegevens stuurt, is iedereen noodzakelijk? Personen van wie je geen reactie verwacht zet je in CC

4 BELEID INZAKE COMMUNICATIE-APPS

Naast email, zijn er tegenwoordig tal van andere communicatieplatformen, ook op mobiele toestellen. Op SmdB De Springplank moedigen we het (professionele, correcte) gebruik van allerhande tools, platformen en apps natuurlijk aan, maar tegelijkertijd willen we iedereen wijzen op het correcte gebruik ervan, en in het bijzonder, ten aanzien van privacygevoelige informatie.

We menen dat medewerkers, ouders en leerlingen verbonden aan SmdB De Springplank hoofdzakelijk een of meerdere van de volgende communicatieplatformen gebruiken:

- Instant messaging via telefonie, zoals bv. SMS, MMS e.d.
- Instant messaging online, zoals bv. (Facebook) Messenger, WhatsApp, Google Hangouts …
- Video-conference, zoals bv. Skype, FaceTime, Google Hangouts, BedNet …

4.1 INTERN BERICHTENSYSTEEM

Voor het beleid en de regels rond het **interne berichtensysteem**, verwijzen we naar het gebruik van de school email-accounts, zoals beschreven in § 3.3.[5]

Elk toestel dat gebruikt wordt om privacygevoelige gegevens uit te wisselen wordt verwacht om beveiligd te zijn met een vergrendeling (zie § 5.2 in het ***toestelbeleid***).

4.2 INSTANT MESSAGING

Deze communicatiekanalen kunnen heel zinvol zijn, ook voor een snel (informeel) werkoverleg, maar binnen SmdB De Springplank is het ten strengste afgeraden om persoonsgegevens van leerlingen te communiceren via een van deze kanalen.

Indien deze kanalen en/of school emailaccounts geraadpleegd worden op een mobiel toestel, vragen wij om dit toestel met een vergrendeling te beveiligen (zie § 5.2 in het ***toestelbeleid***).

4.3 VIDEO CONFERENCING

Ook deze tools zijn zeer interessant, bv. om een overleg van op afstand of met een anders verhinderde collega uit te voeren, maar wees u bewust van:

- de mogelijkheid om in deze tools stem- en/of video-opnames te maken;
- de mogelijkheid om een scherm te delen / over te nemen.

Indien de video-conference een “app” gebruikt op een mobiel toestel, vragen wij om dit toestel met een vergrendeling te beveiligen (zie § 5.2 in het ***toestelbeleid***).

[5] We wijzen er iedereen via deze weg op dat de lokale beheerders van de interne berichtgeving de berichtinhoud van andere gebruikers onmogelijk kunnen lezen.

5 SOCIAL MEDIA-PROTOCOL

Bron: Protocol Sociale Media CSG Het Streek

5.1 INLEIDING

Sociale media zoals Twitter, Facebook, LinkedIn, Instagram, Snapchat, … en nog vele anderen bieden de mogelijkheid te laten zien dat men trots is op de school. Tevens kunnen ze een bijdrage leveren aan een positief imago van SmdB De Springplank.

Het is daarbij van belang te beseffen dat berichten op sociale media (onbewust) de goede naam van de school en betrokkenen ook kunnen schaden. Om deze reden vraagt SmdB De Springplank de aan de school verbonden personen om verantwoord met sociale media om te gaan, de reguliere fatsoensnormen in acht te nemen en de mogelijkheden met een positieve instelling te benaderen.

SmdB De Springplank heeft dit protocol opgezet om aan iedereen die betrokken is, of zich betrokken voelt, richtlijnen te geven. Deze richtlijnen maken een effectieve inzet van sociale media mogelijk. SmdB De Springplank is zich bewust van het feit dat de mogelijkheden van sociale media omvangrijk zijn en dat ze bijna dagelijks veranderen. Om enige toekomstvastheid van dit protocol te borgen zijn de richtlijnen zo generiek als mogelijk omschreven, maar wel getoetst op toepasbaarheid in specifieke situaties.

5.2 UITGANGSPUNTEN

1. SmdB De Springplank onderkent het belang van sociale media.
2. Dit protocol heeft als doel bij te dragen aan een goed en veilig school- en onderwijsklimaat.
3. Dit protocol bevordert dat indien de school, medewerkers, leerlingen en ouders op de sociale media communiceren, dit gebeurt in het verlengde van de missie en visie van de onderwijsinstelling en de reguliere fatsoensnormen. In de regel betekent dit dat we zorgvuldig communiceren, respect voor de school en voor elkaar hebben en iedereen in zijn waarde laten.
4. Het protocol heeft als doel de onderwijsinstelling, de medewerkers, de leerlingen en de ouders te beschermen tegen de mogelijk negatieve gevolgen van sociale media.

5.3 DOELGROEP EN REIKWIJDTE

Deze richtlijnen zijn bedoeld voor alle betrokkenen die deel uitmaken van de “schoolomgeving”, dat wil zeggen medewerkers, leerlingen, ouders/verzorgers en mensen die op een andere manier verbonden zijn aan SmdB De Springplank.

De richtlijnen in dit protocol hebben betrekking op alle op enigerlei wijze aan school of haar medewerkers te relateren berichten.

5.4 SOCIALE MEDIA IN DE SCHOOL

5.4.1 *VOOR ALLE GEBRUIKERS*

1. Het is leerlingen niet toegestaan om tijdens de lessen actief te zijn op sociale media tenzij er op voorhand door een bevoegd personeelslid toestemming is gegeven.
2. Het is medewerkers toegestaan om tijdens de lessen actief te zijn op sociale media zolang dit een onderwijskundige doelstelling heeft.
3. Het is betrokkenen toegestaan om kennis en informatie te delen, mits het geen vertrouwelijke informatie betreft en andere betrokkenen niet schaadt.
4. Ieder is persoonlijk verantwoordelijk voor inhoud die hij of zij publiceert op de sociale media.
5. Elke betrokkene dient zich ervan bewust te zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn en kunnen blijven, ook na verwijdering van het bericht. Dat vraagt om extra zorg en enig voorbehoud bij het plaatsen van berichten.
6. Het is niet toegestaan om foto-, film- en geluidsopnamen van school gerelateerde situaties op sociale media te zetten tenzij de betrokkenen hier uitdrukkelijk toestemming voor hebben gegeven.
7. Op de sociale media waarop geen volledige controle mogelijk is op de berichten die er door anderen worden geplaatst (zoals bv. Facebook) is het medewerkers van SmdB De Springplank afgeraden om privé pagina's en uitingen te delen of het zogenaamde 'vrienden' worden met leerlingen van SmdB De Springplank. De communicatie op deze sociale media vindt plaats via generieke pagina's en profielen (Zie § 5.4.2).

5.4.2 *VOOR MEDEWERKERS IN WERKSITUATIES*

1. Indien het wenselijk is dat er voor een bepaald doel een pagina op sociale media wordt aangemaakt, dan wordt hiervoor een generiek, duidelijk aan school gebonden profiel gebruikt. Het aanmaken van een dergelijke pagina wordt op voorhand met de directe leidinggevende besproken.
2. Elke betrokkene is zich bewust van het feit dat (op sommige sociale media) ook anderen informatie kunnen plaatsen op (profiel) pagina's (tags, linken, posten, etc.).
3. Om die reden zal de eigenaar van de pagina (of topic, discussie, etc.) controlerend optreden en actief redactie voeren op de onder zijn of haar verantwoording aangemaakte pagina's. Zodra de pagina's niet meer nodig zijn worden deze ook door hem of haar weer verwijderd (of non-actief).
4. Medewerkers hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media. Wanneer een medewerker deelneemt aan een discussie of informatie plaatst op een generieke aan school gebonden pagina, dan dient dit in overeenstemming met de officiële standpunten, missie en visie van de onderwijsinstelling te geschieden.
5. Als online communicatie dreigt te ontsporen dient de medewerker direct contact op te nemen met zijn/haar leidinggevende om de te volgen strategie te bespreken.
6. Bij twijfel of een publicatie in strijd is met deze richtlijnen neemt de medewerker contact op met zijn/haar leidinggevende.

5.4.3 *VOOR MEDEWERKERS BUITEN WERKSITUATIES*

Het is medewerkers toegestaan om persoonlijke webpagina's, weblogs, vlogs enz. te onderhouden. Het is daarbij niet toegestaan om aan school gerelateerde onderwerpen te publiceren voor zover het vertrouwelijke of persoonsgebonden informatie over de school, zijn medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen betreft. Een medewerker kan steeds aangesproken worden op berichten, geplaatst op sociale media. Medewerkers moeten zich bewust zijn van hun voorbeeldfunctie.

TOESTELBELEID

vzw SmdB De Springplank

voor:

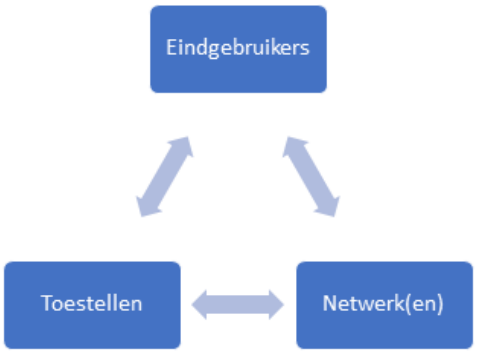
SmdB De Springplank

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB).

Onderwerp	Implementatie - termijn					Implementatie - praktisch	
	OK	25/05/2018	01/09/2018	01/09/2019	Schrappen	Intern	AIV
Logging server/bekabeld netwerk					X	X	
Logging Wifi-netwerk				X		X	
Logging internetverkeer/datagebruik				X		X	
Schooltoestellen: monitoring				X			X
Schooltoestellen: vergrendeling			X			X	
Schooltoestellen: Encryptie/wissen van op afstand (gevoelige geg.)				X			X
Privé-toestellen: vergrendeling			X			X	
Privé-toestellen: anti-virus			X			X	
Privé-toestellen: back-up				X		X	
Privé-toestellen: encryptie/wissen van op afstand (gevoelige geg.)				X		X	
Toepassing wachtwoordbeleid				X		X	

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-03-05	werkdoc	Jasper Vanwalleghem	Markering: invullen school/ instelling/ bestuur adhv 'zoek & vervang' Markering: te bespreken
1.1	2018-03-13	werkdoc	Jasper Vanwalleghem	Toepassen lay-out huisstijl IPCO
1.2	2018-05-15	werkdoc	Jasper Vanwalleghem	Uniformiseren wijzigingen #...#
1.3	2018-07-01	Werkdoc	Jonathan De Laet Karolien Deraeve	Markeringen invullen + overleg
1.4	2018-08-25	Publiek	Jonathan De Laet	Finaliseren voor publicatie

1 INLEIDING



1.1 ALGEMEEN

In een eenvoudige interpretatie zijn er drie aspecten van een modern ICT-netwerk om rekening mee te houden inzake beschikbaarheid, integriteit en vertrouwelijkheid:

- (Eind)gebruikers = *personen*
- Toestellen = *desktops, laptops, maar ook tablets, smartphones, … en ook: servers*
- Netwerk(en) = *de verbinding(en) tussen gebruikers en toestellen*

In deze nota wil SmdB De Springplank enerzijds regels bepalen om de bijdrage van elk van deze drie aspecten in het IVP-beleid te maximaliseren. Anderzijds wordt toegelicht hoe op SmdB De Springplank **controle** op elk van deze aspecten gevoerd wordt.

Deze nota valt onder de eindverantwoordelijkheid van vzw SmdB De Springplank.

1.2 ALGEMENE BEPALINGEN

Ongeacht het “type” toestel of netwerk, zijn er een aantal maatregelen die SmdB De Springplank steeds toepast. Hieronder worden deze opgesomd. In wat volgt, worden de specifieke maatregelen toegelicht.

- Het combineren met een aantal monitoring tools en/of logboeken, d.w.z. manieren om de handelingen bij te houden voor analyse of eventueel naar bewijslast toe.
- In deze logboeken worden een aantal **identificatieparameters** geregistreerd. Er vindt geen ongeoorloofde inzage of systematische analyse plaats op deze gegevens. Enkel bij gegronde vermoedens van inbreuken kunnen hierop gerichte en/of willekeurige controles uitgevoerd worden. Alle informatie hier aangaande wordt strikt vertrouwelijk behandeld.

2 NETWERKBEVEILIGING EN -CONTROLE

2.1 BEKABELD NETWERK EN SERVERS

Met het “bekabelde netwerk” bedoelen we het geheel van componenten die de netwerkverbindingen maken en beheren, zoals: routers, switchen, printers, kabels, servers …

De algemene maatregelen (zie § 1.2) worden toegepast, waaronder mogelijk de logging van: tijdsregistratie, MAC/IP-adressen, toestelnamen, gebruikersnamen.

Wachtwoorden op de netwerkcomponenten worden bij installatie gewijzigd (geen ‘default’ waarden). De gekozen wachtwoorden voldoen aan het ***wachtwoordbeleid***.

2.2 WIFI-NETWERK

Voor personeel, leerlingen en gasten is wifi voorzien en/of mogelijk op SmdB De Springplank. Deze dienst is gratis voor de eindgebruikers, maar heeft voor de school wel een zekere kostprijs (in aanschaf, onderhoud en beveiliging).

Daarom wordt in de mate van het mogelijke de aard en hoeveelheid van het netwerkverkeer gemonitord.

De algemene maatregelen (zie § 1.2) worden toegepast, waaronder mogelijk de logging van: tijdsregistratie, MAC/IP-adressen, toestelnamen, gebruikersnamen.

Ook de bezochte websites of applicaties, en het datagebruik via het draadloze netwerk, wordt waar mogelijk bijgehouden in logboeken en kan desgevallend wel geanalyseerd worden, als het globale verbruik (bv. misbruik) dit rechtvaardigt. Alle informatie hier aangaande wordt strikt vertrouwelijk behandeld.

Het netwerkverkeer dat via het draadloze netwerk verloopt, wordt normaal gezien *niet* versleuteld. Het werken met persoonsgegevens via dit netwerk wordt dan ook ten stelligste afgeraden. Zonder veel moeite kunnen andere gebruikers op het netwerk meekijken… tenzij er een andere vorm van versleuteling gehanteerd wordt (*bv. https i.p.v. http*).

3 BEVEILIGING & CONTROLE INTERNETVERKEER

Op SmdB De Springplank is er, zowel voor de toestellen die eigendom zijn van de school als op bepaalde andere toestellen (zie ook § 2.2, § 4 en § 5), een internetverbinding mogelijk.

Als organisatie is SmdB De Springplank verantwoordelijk voor het algehele dataverbruik, en voor alles wat er met of via deze internetverbinding gebeurt. Daarom hanteert men ook hier een aantal regels en controles daarop:

De algemene maatregelen (zie § 1.2) worden toegepast, waaronder mogelijk logging van: tijdsregistratie, MAC/IP-adressen, toestelnamen, gebruikersnamen.

De beheerders, noch de elektronische controlesystemen en de logboeken, hebben op geen enkele manier toegang tot de inhoud van persoonlijke berichten (zoals messaging, email, intern communicatiesysteem, …).

4 BEVEILIGING EN CONTROLE OP TOESTELLEN VAN DE SCHOOL

Onder “toestellen” van de school rekenen we zowel desktop computers, laptops, tablets als (eventuele) werk-smartphones die eigendom zijn van de school. Ook andere geconnecteerde toestellen vallen hier onder.

4.1 ALGEMEEN

De volgende beveiligingsregels resp. -controles kunnen hierop (tegelijkertijd) toegepast worden:

- Het internetverkeer en gebruikte toepassingen wordt, op verscheidene niveaus, gecontroleerd inzake bv. bezochte doelsites, uitgaand verkeer, capaciteit maar ook veiligheid van de toepassing, het al dan niet veranderen van systeeminstellingen (gerelateerd aan beveiliging resp. prestaties, enz.)
- De beheerders steken veel tijd en geld in het zo vlot mogelijk “draaiend” houden van alle hardware en het netwerk. Dit is onmogelijk als gebruikers de systeem- of beveiligingsinstellingen veranderen. Er worden op SmdB De Springplank dan ook verschillende maatregelen genomen om dit te verhinderen. Het doelbewust veranderen van systeem- of beveiligingsinstellingen is verboden.
- Op SmdB De Springplank worden er bepaalde tools gebruikt die de actieve vensters en/of het real-time beeldscherm van de eigen toestellen kunnen monitoren. De doeleinden hiervan zijn louter en alleen pedagogisch. Het is bijvoorbeeld leerkrachten en ondersteunend personeel *niet* toegestaan om zonder concreet vermoeden van doelbewuste en ernstige inbreuken, schermafdrukken te bewaren, een scherm op te nemen of een scherm over te nemen zonder toestemming van de betrokkene.
- Leerkrachten en ondersteunend personeel kunnen, in het kader van hun uit te oefenen taak, de actieve vensters, geopende websites en/of het beeldscherm zien. Het is niet uitgesloten dat de inhoud van **persoonlijke berichten** (ontvangen en/of verzonden) leesbaar is, alhoewel dit nooit het doel op zich zal zijn. Al deze medewerkers behandelen de informatie strikt vertrouwelijk, en bewaren deze niet.
- Het is, met dezelfde tools, wel toegestaan dat de beheerders, directie en eventueel andere personeelsleden die hiervoor bevoegd geacht worden, de schermen bewaren (als een schermafdruk of als een opname). Zij doen dit enkel bij een concreet vermoeden van doelbewuste en ernstige inbreuken en alle informatie wordt strikt vertrouwelijk behandeld. Onbevoegde medewerkers hebben geen toegang tot de schermafdrukken of opnames.

Dit beleid wordt waar mogelijk gecombineerd met een aantal monitoring tools en/of (lokale) logboeken, d.w.z. manieren om de handelingen bij te houden voor analyse of eventueel naar bewijslast toe. De algemene maatregelen (zie § 1.2) worden toegepast, waaronder mogelijk logging van: tijdsregistratie, MAC/IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen.

4.2 VERGRENDELING, ENCRYPTIE, WISSEN VAN OP AFSTAND

De mobiele toestellen (laptops, pda's, tablets, smartphones…) die bepaalde personeelsleden gebruiken maar die eigendom zijn van SmdB De Springplank, dienen extra beveiligd te worden indien er persoonsgegevens op bewaard, bekeken of verwerkt worden.

Er wordt een vergrendeling a.d.h.v. wachtwoord, pincode, swipe code, vingerafdruk en/of andere authenticatiemanier toegepast.

Voor directie, ondersteunend personeel dat toegang heeft tot gevoelige persoonsgegevens op het toestel in kwestie, zorgverantwoordelijken en CLB geldt bovendien: indien mogelijk encrypteren van opslagmedia.

5 BEVEILIGING EN CONTROLE OP TOESTELLEN VAN EINDGEBRUIKERS ZELF

Op SmdB De Springplank is het mogelijk om, via het netwerk of wifi van de school (zie ook § 2), gebruik te maken van eigen toestellen. Het is de bedoeling dat deze maximaal gebruikt worden om taken uit te voeren, gerelateerd aan de onderwijsinstelling.

5.1 ALGEMEEN

Inzake een eigen toestel zijn een aantal beveiligings- en beheerdersaspecten anders dan in § 4. Toch gelden alle principes van deze paragraaf evenzeer voor handelingen gerelateerd aan SmdB De Springplank, die uitgevoerd worden op een eigen toestel. Zie, naast § 4 uit deze nota, ook het algemene ***communicatiebeleid***. De bijzondere regels en afspraken inzake het BYOD[6]-beleid, zijn:

- Het gebruik van een eigen toestel voor de aan de school gerelateerde processen op het netwerk van de school is enkel toegestaan wanneer het doel van gebruik niet kan bereikt worden met een toestel van de school.
- De gebruiker is volledig verantwoordelijk en staat zelf in voor de veiligheid van de programmatuur op zijn toestel. Zie § 5.2.
- Wanneer onbevoegde programmatuur op het toestel van de gebruiker zonder medeweten van de gebruiker zelf ongeoorloofde acties uitvoert met persoonsgegevens dan is de gebruiker zelf hiervoor ten volle aansprakelijk.

Het internetverkeer en gebruikte toepassingen wordt, waar mogelijk en op verscheidene niveaus, gecontroleerd inzake bv. bezochte doelsites, uitgaand verkeer, capaciteit maar ook veiligheid van de toepassing… De algemene maatregelen (zie § 1.2) worden ook toegepast, waaronder mogelijk logging van: MAC/IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen...

[6] BYOD = "bring your own device". Het gebruik van eigen toestellen op en voor schoolgerelateerde processen.

5.2 VERGRENDELING, ENCRYPTIE, ANTIVIRUSBEVEILIGING, BACKUPS EN WISSEN VAN OP AFSTAND

De mobiele toestellen (d.w.z. laptops, pda's, tablets, smartphones) van medewerkers, waarop persoonsgegevens van SmdB De Springplank bewaard, bekeken of verwerkt worden, dienen extra beveiligd te worden. Dit beleid vraagt die medewerkers dan ook om de volgende maatregelen op deze toestellen in acht te nemen:

- Er wordt een vergrendeling a.d.h.v. wachtwoord, pincode, swipe code, vingerafdruk of andere authenticatie gevraagd.
- Er wordt gevraagd om een ten allen tijde up-to-date antivirusprogramma te gebruiken.
- Backups dienen genomen, bewaard en beheerd te worden zoals in het respectievelijke beleid vastgelegd. Hou hierbij rekening met het feit dat bepaalde gegevens niet langer mogen bijgehouden worden dan nodig/nuttig voor de school.
- Voor directie, ondersteunend personeel dat toegang heeft tot gevoelige persoonsgegevens op het toestel in kwestie, zorgverantwoordelijken en CLB wordt daarenboven het volgende gevraagd: indien mogelijk encrypteren van opslagmedia.

BACKUPBELEID

vzw SmdB De Springplank

voor:

SmdB De Springplank

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB).

Onderwerp	Implementatie - termijn					Implementatie - praktisch	
	OK	25/05/2018	01/09/2018	01/09/2019	Schrappen	Intern	AIV
Stroomvoorziening				X		X	
Alternatieve internetverbinding					X		X
Backups				X		X	
Brandveiligheid				X			X

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-03-05	werkdoc	Jasper Vanwalleghem	Markering: invullen school/ instelling/ bestuur adhv 'zoek & vervang' Markering: te bespreken
1.1	2018-03-13	werkdoc	Jasper Vanwalleghem	Toepassen lay-out huisstijl IPCO
1.2	2018-05-15	werkdoc	Jasper Vanwalleghem	Uniformiseren wijzigingen #...#
1.3	2018-07-01	Werkdoc	Jonathan De Laet Karolien Deraeve	Markeringen invullen + overleg
1.4	2018-08-25	Publiek	Jonathan De Laet	Finaliseren voor publicatie

1 INLEIDING

1.1 SITUERING

Voor de gegevens die een bepaald niveau van beschikbaarheid en/of integriteit vereisen, is een goed uitgestippeld backupbeleid noodzakelijk. Deze principes gelden zowel voor gegevens die zich op NAS-en, servers, clients, eigen toestellen, andere locaties, in de cloud, … bevinden – zie ook het ***toestelbeleid*** en het BYOD-beleid in § 5 in het bijzonder.

Zie de ***classificatie van gegevens*** voor meer info aangaande de gehanteerde BIV-niveau's.

Deze nota valt onder de eindverantwoordelijkheid van vzw SmdB De Springplank.

1.2 ENKELE BEGRIPPEN

UPS (uninterrupted power supply) Noodstroom-voorziening	Aangesloten systemen en opslagmedia worden gedurende enkele minuten van stroom voorzien bij pannes of spanningsfluctuaties. Dit zorgt ervoor dat gegevens in het werkgeheugen en/of cache nog kan weggeschreven worden voordat het system afgesloten moet worden.
Redundantie	Het algemene principe waarbij een systeem, opslag of netwerkverbinding zo opgebouwd wordt, dat indien nodig een ander systeem overneemt. In principe mogen eindgebruikers hier niets van merken. Het "eerste" systeem dient zo snel mogelijk terug hersteld te worden.
Backups	Het nemen van geregelde kopieën, op een andere locatie en medium, zodat bij eventueel verlies of diefstal de gegevens in kwestie hersteld kunnen worden. De aard, frequentie, enz. van de backups wordt bepaald door de classificatie van de gegevens in kwestie. Dit proces kan volledig geautomatiseerd gebeuren.
Synchronisatie	Gegevens bevinden zich op verschillende locaties en media, maar een onderlinge netwerkverbinding zorgt ervoor dat beide kopieën hetzelfde zijn. Aanpassingen gebeuren m.a.w. steeds in beide kopieën tegelijk. Het systeem zorgt ervoor dat aanpassingen bijgehouden worden in het geval dat de verbinding (even) weg valt, om deze bij het herstellen van de verbinding zo snel mogelijk samen te voegen.

2 STROOMVOORZIENING

Alle systemen waarop gegevens gebruikt of bewaard worden die behoren tot het beschikbaarheidsniveau ***noodzakelijk*** en/of het integriteitsniveau ***absoluut***, worden in SmdB De Springplank voorzien van een noodstroomvoorziening.

Gegevens die behoren tot het beschikbaarheidsniveau ***belangrijk*** en/of het integriteitsniveau ***vereist***, worden indien mogelijk voorzien van een noodstroomvoorziening.

3 INTERNETVERBINDING

Alle systemen waarvoor een (voldoende snelle) internetverbinding nodig is, en die behoren tot het beschikbaarheidsniveau ***noodzakelijk*** en/of het integriteitsniveau ***absoluut***, worden in SmdB De Springplank voorzien van een internetverbinding, met noodstroomvoorziening.

Indien mogelijk, worden voor deze systemen SLA's afgesloten met de ISP('s) in kwestie (kwaliteits- en verbindingsgaranties).

4 BACKUPS

Gegevens die behoren tot het beschikbaarheidsniveau ***belangrijk*** en/of het integriteitsniveau ***vereist***, worden minstens wekelijks geback-upt.

Alle andere gegevens die belangrijk zijn voor de werking van de school worden wekelijks geback-upt.

Minstens één keer per schooljaar vindt een volledige back-up van alle gegevens plaats, behoudens de gegevens die niet verder (in een archief) bewaard (mogen) worden.

Alle back-ups worden conform de gangbare "best practices" bewaard en (persoons)gegevens die behoren tot het vertrouwelijkheidsniveau ***vertrouwelijk*** of ***geheim***, worden geëncrypteerd geback-upt.

5 BRANDVEILIGHEID

De fysieke plaatsen op SmdB De Springplank waar geback-upte gegevens bewaard worden is verschillend van de fysieke plaats vanwaar de gegevens komen in functie van het veiligheidsplan.

Indien deze gegevens (ook) bewaard worden op een andere locatie en/of bij (een) externe verwerker(s), dan legt vzw SmdB De Springplank hieraan gelijkaardige eisen op.