

# INFORMATIEVEILIGHEIDS- EN PRIVACYBELEID



VOOR:

**Basisonderwijs Dominiek Savio** (inst. nr. 26741)

**Secundair Onderwijs Dominiek Savio** (inst. nr. 28134)

Versie	Datum	Status	Opmerking
1.0	30/05/2018	ONTWERP	Besproken met CIV op 2/03/2018
1.1	05/06/2018	GOEDGEKEURD	Goedgekeurd door Raad van Bestuur

## Inhoud

Afkortingen.....	3
1 Inleiding.....	4
1.1 Toelichting informatieveiligheid.....	4
1.2 Toelichting privacy.....	4
1.3 Vervlechting informatieveiligheid en privacy.....	5
2 Doel en reikwijdte.....	5
2.1 Doel.....	5
2.2 Reikwijdte.....	5
3 Uitgangspunten.....	6
3.1 Algemene beleidsuitgangspunten.....	6
3.2 Uitgangspunten privacy.....	7
4 Wet- en regelgeving.....	8
5 Organisatie.....	8
5.1 Rollen (functies) rondom IVP.....	9
5.2 Richtinggevend.....	9
5.3 Sturend.....	9
5.4 Sturend + uitvoerend.....	10
5.5 Uitvoerend.....	10
6 Controle en rapportage.....	11
6.1 Voorlichting en bewustzijn.....	12
6.2 Classificatie en risicoanalyse.....	12
6.3 Incidenten en datalekken.....	12
6.4 Controle, naleving en sancties.....	12
Bijlage 1: Tabel IVP rollen en taken.....	13
Bijlage 2: Aanvullende nota's.....	15

## Afkortingen

AVG = Algemene Verordening Gegevensbescherming

IVP = Informatieveiligheid en privacy

IVPB = Informatieveiligheids- en privacybeleid

MFC = Multifunctioneel Centrum

DPO = Data Protection Officer

AIV = Aanspreekpunt Informatieveiligheid

GEB = Gegevensbeschermingseffectbeoordeling

CIV = Cel voor Informatieveiligheid

CAO = Collectieve Arbeidsovereenkomst

SLA = Service Level Agreement

ISP = Internet Service Provider

## 1 Inleiding

Informatie en ICT zijn noodzakelijk in de ondersteuning van het onderwijs. Denken we maar aan de leerlingenadministratie- en leerlingvolgsystemen, agenda- en rapportprogramma's, oefen- en toetsystemen, personeelsadministratie, ... Vaak verwerken deze geautomatiseerde systemen persoonsgegevens (van leerlingen, ouders, personeel, ...) 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 aan te pakken is het noodzakelijk dat we een duidelijk beleid opstellen om duidelijk te maken waar het om gaat, een doel stellen en de manier vastleggen 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 imagooverlies.

### 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 en 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 Dominiek Savio Onderwijs.

## 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 Dominiek Savio Onderwijs.
- 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, beschikbare tijd en middelen. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkenen, met name van (oud)leerlingen, ouders, (ex)medewerkers en derden wordt gerespecteerd en dat Dominiek Savio Onderwijs voldoet aan relevante wet- en regelgeving.

### 2.2 Reikwijdte

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Dominiek Savio Onderwijs waaronder in ieder geval: alle (ex)medewerkers, (oud)leerlingen, ouders/verzorgers, vrijwilligers, stagiairs, (geregistreerde) bezoekers en externe relaties, evenals op andere betrokkenen waarvan Dominiek Savio Onderwijs persoonsgegevens verwerkt.
- Dit beleid is van toepassing op zowel de digitale als de geschreven verwerking van persoonsgegevens.
- Het IVP-beleid geldt voor alle medewerkers, leerlingen, ouders/verzorgers, vrijwilligers, stagiairs (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 de school 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 beleid zal worden aangevuld met concrete procedures en/of checklists rond bv. hoe omgaan met vragen over IVP, hoe omgaan met datalekken, procedure rond verwisselbare media, enz.
- Het IVP-beleid binnen Dominiek Savio Onderwijs heeft raakvlakken met:
  - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten het intern noodplan, fysieke toegang en beveiliging, bedrijfshulpverlening (EHBO voor werknemers) en ongevallen;
  - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties;
  - ICT-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.
  - Het IVP-beleid van het Beleidsdomein Zorg binnen Dominiek Savio, waar Dominiek Savio Onderwijs een nauw samenwerkingsverband mee voert.

## 3 Uitgangspunten

### 3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Dominiek Savio Onderwijs 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:

- de verwerkingsverantwoordelijke moet een wettelijke verplichting nakomen
- de verwerkingsverantwoordelijke moet een overeenkomst met de betrokkene nakomen
- er is een vitaal belang van de betrokkene
- er moet een taak van openbaar belang uitgevoerd worden
- er is een gerechtvaardigd belang voor de verwerkingsverantwoordelijke
- de betrokkene heeft de verwerkingsverantwoordelijke toestemming gegeven

Hierbij willen we een goede balans zoeken tussen het belang van Dominiek Savio Onderwijs 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, Dominiek Savio vzw, is als rechtspersoon de **verwerkingsverantwoordelijke** voor alle persoonsgegevens die in opdracht van Dominiek Savio Onderwijs verwerkt worden.

- Dominiek Savio Onderwijs 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 Dominiek Savio Onderwijs 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.
- Dominiek Savio Onderwijs sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) **verwerkersovereenkomsten** af indien deze persoonsgegevens ontvangen van de school.
- Binnen Dominiek Savio Onderwijs 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, vrijwilligers, stagiairs, (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 imagooverlies. In het *algemeen reglement van het personeel van het katholiek onderwijs* (artikel 7 § 7) wordt hiernaar verwezen.
- Bij wijzigingen in de infrastructuur, de aanschaf en de uit dienst name van (informatie)systemen, wordt bij Dominiek Savio Onderwijs steeds rekening gehouden met IVP.
- IVP is bij Dominiek Savio Onderwijs een continu proces, ingebed in ons kwaliteitssysteem en waar jaarlijks werkdoelen voor kunnen bepaald worden.

### 3.2 Uitgangspunten privacy

De zeven vuistregels met betrekking tot de omgang van persoonsgegevens bij Dominiek Savio Onderwijs zijn:

1. **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. (zie 3.1)
2. **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.
3. **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.

4. **Databeperking:** 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.
5. **Opslagbeperking:** data wordt niet langer bewaard dan noodzakelijk. De verwerking wordt door het IVP-beleid beperkt in de tijd.
6. **Juistheid:** 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 Dominiek Savio Onderwijs te waarborgen.
7. **Veiligheid en vertrouwelijkheid:** persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen. Het uitgangspunt voor toegang tot persoonsgegevens is Privacy by Default: standaard heeft niemand toegang.

Bij alle registraties op basis van **toestemming**, zal Dominiek Savio Onderwijs een eenduidige procedure hanteren die een actieve en aantoonbare handeling vereist.

## 4 Wet- en regelgeving

Dominiek Savio Onderwijs voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Algemene Verordening Gegevensbescherming (AVG)
- 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 Dominiek Savio Onderwijs 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 Dominiek Savio Onderwijs een aantal rollen aan medewerkers in de bestaande organisatie toegewezen.

## 5.2 Richtinggevend

### **Verwerkingsverantwoordelijke**

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

De evaluatie van de toepassing en werking van het IVP-beleid wordt ingebed in ons kwaliteitssysteem en jaarlijks gerapporteerd aan de Raad van Bestuur.

Zie bijlage 1 voor een schematische weergave van de rol- en taakverdelingen aangaande IVP op Dominiek Savio Onderwijs en binnen Dominiek Savio vzw.

## 5.3 Sturend

### **Data Protection Officer (DPO) van de koepelorganisatie**

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 (GEB);
- Met de toezichthoudende autoriteit samenwerken en optreden als aanspreekpunt voor deze autoriteit.

### **Aanspreekpunt Informatieveiligheid**

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:

- Directie/bestuur en personeel informeren en adviseren over IVP
- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- Meewerken aan de bewustmaking en opleiding van het personeel
- De uniformiteit bewaken binnen Dominiek Savio Onderwijs
- Het register voor verwerkingsactiviteiten invullen en actualiseren
- Advies verstrekken over de verwerkersovereenkomsten
- Een gegevensbeschermingseffectbeoordeling uitvoeren voor het leerlingvolgsysteem
- Meewerken aan de classificatie van persoonsgegevens, risicoanalyse en het opstellen van een

veiligheidsplan

- Het aanspreekpunt zijn voor vragen, meldingen en incidenten op het gebied van IVP
- De verdere afhandeling van incidenten binnen Dominiek Savio Onderwijs coördineren
- Optreden als contactpersoon voor de toezichhoudende autoriteit en de informatieveiligheidsconsulent van de koepel.

## 5.4 Sturend + uitvoerend

### **Cel voor Informatieveiligheid**

Het aanspreekpunt informatieveiligheid kan bovenstaande taken niet alleen uitvoeren. Daarom is er binnen Dominiek Savio Onderwijs een Cel voor informatieveiligheid (CIV) opgericht. Deze cel bestaat uit personen die verantwoordelijk zijn voor onder andere personeelsdienst, financiën, leerlingenadministratie, ICT, leidinggevend en het aanspreekpunt informatieveiligheid. De diverse samenstelling van deze CIV-werkgroep helpt mee om een brede kijk te krijgen op de verschillende processen waar persoonsgegevens binnen de onderwijscontext verwerkt worden. Daarnaast helpt de CIV met de implementatie van de verordening op school.

De CIV geeft advies bij en/of werkt mee aan:

- Het opmaken van een inventaris van alle persoonsgegevens die worden verwerkt
- Het uitvoeren van een algemene risicoanalyse
- Het IVP-beleid
- Het formuleren van een voorstel tot toegangsrechten
- De classificatie van persoonsgegevens en toegangsmatrices
- Het opstellen van de verwerkersovereenkomsten
- De privacyverklaring en de communicatie met de betrokkenen
- De beveiligingsprotocollen
- De toestemmingen en het toestemmingbeheer

Het opvolgingsproces voor IVP wordt ook uitgevoerd door de CIV, in opdracht van het schoolbestuur.

## 5.5 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 op Dominiek Savio Onderwijs zijn beschreven in o.a. dit informatieveiligheids- en privacybeleid en de eraan toegevoegde nota's. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met procedures, checklists, formulieren en praktische tools.

Medewerkers worden 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 Dominiek Savio Onderwijs die toegang kunnen hebben tot persoonsgegevens, gebonden aan een discretieplicht<sup>1</sup>. Welbepaalde (externe) medewerkers zijn wettelijk gebonden aan een beroepsgeheim<sup>2</sup>.

## 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 Dominiek Savio Onderwijs een 2-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 de bestaande overlegvormen.

---

<sup>1</sup> Discretieplicht is de verplichting om bij het uitoefenen van een functie of ambt geen gegevens vrij te geven aan anderen dan wie recht heeft op die gegevens. Iedereen die in een school werkt, heeft discretieplicht (ambtsgeheim). Schoolpersoneel mag vertrouwelijke informatie over leerlingen discreet bespreken met collega's, directie of het CLB om zo de leerlingen de nodige ondersteuning te bieden. Met derden die buiten de onderwijsinstelling staan, mag dat niet.

<sup>2</sup> Beroepsgeheim is de geheimhoudingsplicht die van toepassing is op wie vanwege staat of beroep geheimen kent die hem zijn toevertrouwd. Bv. CLB-medewerkers hebben beroepsgeheim. Zij mogen enkel in het belang van de leerling aan het betrokken schoolpersoneel gegevens bezorgen als ze die informatie nodig hebben om hun taak goed te vervullen in functie van de leerling.

(Bron: Klasse.be, Anne Siccard, 18/01/2018, <https://www.klasse.be/42288/als-leraar-beroepsgeheim/>)

## 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 Dominiek Savio Onderwijs 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 Dominiek Savio vzw als eindverantwoordelijke.

## 6.2 Classificatie en risicoanalyse

Bij Dominiek Savio Onderwijs 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 Dominiek Savio Onderwijs is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Alle incidenten kunnen worden gemeld bij [privacy@dominieksavio.be](mailto:privacy@dominieksavio.be). 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 hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Dominiek Savio Onderwijs wordt actief aandacht besteed aan IVP bij de aanstelling, tijdens functioneringsgesprekken, met procedures, met een communicatieplan, met periodieke bewustwordingscampagnes, et cetera.

Mocht de naleving ernstig tekort schieten, dan kan Dominiek Savio vzw 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.

## Bijlage 1: Tabel IVP rollen en taken

Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Schoolbestuur	<ul style="list-style-type: none"> <li>Eindverantwoordelijke</li> <li>IVP-beleidsvorming, -vastlegging en het uitdragen ervan</li> <li>Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens</li> <li>Evalueren toepassing en werking IVP-beleid op basis van rapportages en bijsturen van dit beleid indien nodig</li> <li>Organisatie IVP inrichten</li> </ul>	<ul style="list-style-type: none"> <li>Informatieveiligheids- en privacy beleid opstellen, goedkeuren en communiceren</li> <li>Aanspreekpunt informatieveiligheid aanstellen</li> <li>Oprichten veiligheidscel</li> </ul>
Leidinggevende (directie)	<ul style="list-style-type: none"> <li>Toeziens op de naleving van het IVP-beleid en privacywetgeving en de daarbij behorende processen, richtlijnen en procedures door de medewerkers.</li> <li>Communicatie naar alle betrokkenen; er voor zorgen dat alle medewerkers op de hoogte zijn van het IVP-beleid en de consequenties ervan.</li> <li>Voorbeeldfunctie met positieve en actieve houding t.a.v. IVP-beleid.</li> <li>Rapporteren voortgang m.b.t. doelstellingen IVP-beleid aan bestuur</li> <li>Periodiek het onderwerp informatieveiligheid onder de aandacht brengen in werkoverleg, beoordelingen,...</li> <li>Implementeren IVP-maatregelen.</li> </ul>	<p>Communiceren, informeren en toezien op naleving van o.a.:</p> <ul style="list-style-type: none"> <li>IVP in het algemeen</li> <li>Hoe omgaan met leerlingendossiers</li> <li>Wie mag wat zien</li> <li>Gedragscode</li> <li>Beveiliging van ruimtes</li> <li>Preventieve maatregelen ( o.a. brand en waterschade aan servers...)</li> <li>...</li> </ul>
Data Protection Officer (DPO) koepel	<ul style="list-style-type: none"> <li>Schoolbesturen informeren en adviseren over hun verplichtingen krachtens de AVG en regelgeving;</li> <li>Richtlijnen, kaders, procedures opstellen en aanbevelingen doen m.b.t. informatieveiligheid en privacy</li> <li>Aanspreekpunten IVP opleiden en hen de nodige tools en hulpmiddelen verstrekken</li> <li>Desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling</li> <li>Samenwerken met de toezichhoudende autoriteit en optreden als aanspreekpunt voor deze autoriteit</li> <li>Brugfiguur naar de externe partijen toe</li> <li>Lerend netwerk ontwikkelen en aansturen</li> </ul>	<ul style="list-style-type: none"> <li>Opstellen van algemene processen, richtlijnen en sjablonen IVP</li> <li>Nascholingstraject organiseren</li> <li>Overleg met informatieveiligheidsconsulenten onderwijsnetten en GO!</li> <li>Overleg met externe partijen: leveranciers van leerlingadministratie en -volgsystemen en leveranciers van didactische software</li> <li>Tools aanpassen/ontwikkelen</li> </ul>

Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Aanspreekpunt informatieveiligheid	<ul style="list-style-type: none"> <li>• Informeert en adviseert directie/bestuur en personeel over IVP</li> <li>• Rapporteert naar directie/bestuur</li> <li>• Informeert de data protection officer van de koepel</li> <li>• Meewerken aan de uitwerking van een IVP-beleid</li> <li>• Voorstellen doen tot aanpassingen van centraal aangeboden processen, richtlijnen en procedures om de uitvoering van het IVP-beleid te ondersteunen binnen de school</li> <li>• Meewerken aan: <ul style="list-style-type: none"> <li>○ classificatie van middelen</li> <li>○ risicoanalyse</li> <li>○ het opstellen van een veiligheidsplan</li> </ul> </li> <li>• Aanspreekpunt voor vragen, meldingen en incidenten ivm IVP</li> <li>• Incidentafhandeling (registreren en evalueren).</li> <li>• Invullen register verwerkingsactiviteiten</li> </ul>	<p>Voorstellen van aanpassingen aan de uitgewerkte formulieren van processen, richtlijnen en procedures rond IVP, bijvoorbeeld:</p> <ul style="list-style-type: none"> <li>• Security awareness activiteiten</li> <li>• Authenticatie en autorisatie-beleid</li> <li>• Gedragscodes (ICT en internetgebruik, sociale media, privacybeleid...) naar medewerkers en leerlingen toe</li> <li>• Verwerkersovereenkomsten regelen</li> <li>• Toestemming opstellen gebruik foto's en video</li> <li>• Communicatieplan naar medewerkers, leerlingen, ouders en cursisten</li> <li>• Procedure IVP-incident afhandeling</li> <li>• Inrichten meldpunt datalekken</li> <li>• Melden datalekken naar de overheid toe</li> <li>• ...</li> </ul> <p>Invullen van register verwerkingsactiviteiten voor schooleigen situatie</p>
Informatieveiligheids cel (CIV) van de school <sup>3</sup>	<ul style="list-style-type: none"> <li>• Classificatie van informatie</li> <li>• IVP risicoanalyse uitvoeren</li> <li>• Prioriteiten voorstellen</li> <li>• Toegangsbeleid zowel fysiek als digitaal vaststellen en laten bekrachtigen door bestuur</li> <li>• De toegangsrechten van gebruikers regelmatig beoordelen en controleren.</li> <li>• Adviseren bij en mee uitwerken van het IVP-beleid</li> <li>• Evalueren IVP-beleid en voorstellen van verbetermaatregelen</li> <li>• Bespreking veiligheidsincidenten en voorstellen formuleren voor te nemen maatregelen</li> <li>• Aanpassen gegevensbeschermingseffectbeoordeling aan eigen situatie</li> </ul>	<ul style="list-style-type: none"> <li>• Inventariseren waar persoonsgegevens van de school terecht komen (leveranciers lijst)</li> <li>• Classificatie van informatiebronnen en persoonsgegevens</li> <li>• Risicoanalyse uitvoeren en documenteren</li> </ul> <p>Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder:</p> <ul style="list-style-type: none"> <li>• Toegangsmatrix diverse informatiesystemen en netwerk</li> </ul>
Iedereen	<ul style="list-style-type: none"> <li>• Uitvoeren taken conform gegeven richtlijnen en procedures.</li> <li>• Verantwoordelijk omgaan met IVP bij de dagelijkse werkzaamheden</li> </ul>	<p>Richtlijnen en procedures volgen</p> <p>Melden van vragen en incidenten aan aanspreekpunt informatieveiligheid</p>

<sup>3</sup> bestaande uit de verantwoordelijken voor bv. ICT, personeelsdienst, preventieadviseur, financiën, leerlingenadministratie, facilitair management, leidinggevende en het aanspreekpunt informatieveiligheid

## 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
- Back-upbeleid

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

# CLASSIFICATIE VAN PERSOONSgegevens



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

VOOR:

**Basisonderwijs Dominiek Savio** (inst. nr. 26741)

**Secundair Onderwijs Dominiek Savio** (inst. nr. 28134)

Versie	Datum	Status	Opmerking
1.0	30/05/2018	ONTWERP	Besproken met CIV op 20/03/2018 en 27/04/2018
1.1	05/06/2018	GOEDGEKEURD	Goedgekeurd door Raad van Bestuur



## 1 Inleiding

### 1.1 Situering

Door een classificatie van persoonsgegevens te maken, kan men op Dominiek Savio Onderwijs 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 Dominiek Savio Onderwijs de nodige organisatorische en technische maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid gepast te waarborgen.

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB) en valt onder de eindverantwoordelijkheid van Dominiek Savio vzw.

### 1.2 Hoe wordt het classificatieniveau bepaald?

Dit doen we op Dominiek Savio Onderwijs 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 Dominiek Savio Onderwijs de onderstaande categorieën van persoonsgegevens.

#### 1.3.1 Leerlingen

- Rijksregister: *rijksregisternummer*
- Identificatie: *voornaam, naam, geboortedatum, geboorteplaats en/of identiteitskaartnummer*
- Indicatoren: *heeft moeder diploma/getuigschrift secundair onderwijs, anderstalig thuis, broer/zus, ouder(s) personeel, studietoelage ontvangen 2 voorbije schooljaren*
- Pasfoto: *zoals op identiteitskaart, zelf genomen of via schoolfotograaf*
- Contact (school): *vast telefoonnummer, e-mailadres v.d. school, gsm-nummer v.d. school*
- Contact (privé): *eigen vast telefoonnummer, eigen e-mailadres, eigen gsm-nummer*
- Schoolloopbaan: *instellingen, jaren, richtingen, klassen*
- Afwezigheden: *afwezige (halve) dagen, redenen, bewijzen*

- Evaluatie: *puntenboeken, remediëring, rapporten, commentaren, deliberaties, verslagen, eindbeslissingen, motiveringen*
- Functioneren: *gedrag, welbevinden, communicatie met leerkrachten, medeleerlingen, groepsdynamiek, begeleiding, medische informatie (nodig om het kind te begeleiden en te onderwijzen), opvolging, straffen, sancties, tucht*
- Medische informatie: *zoals beschreven in wetgeving, incl. zorgdiagnoses, -dossiers en medische begeleiding. Medische informatie die voor leerkrachten nodig is om de leerling te onderwijzen en begeleiden, valt onder 'functioneren' (bv. gedragsmaatregelen, sticordi-maatregelen)*

### 1.3.2 Ouder(s) / voogd

- Identificatie: *voornaam, naam, geboortedatum, geboorteplaats en/of identiteitskaartnummer*
- Adres: *straat, nummer, busnummer, postcode, gemeente, deelgemeente, land*
- Contact (privé): *eigen vast telefoonnummer, eigen e-mailadres, eigen gsm-nummer*
- Financieel: *bankgegevens, betaalde rekeningen, openstaande rekeningen, afbetalingen*

### 1.3.3 Personeel

- Rijksregister: *rijksregisternummer*
- Identificatie: *voornaam, naam, geboortedatum, geboorteplaats en/of identiteitskaartnummer*
- Pasfoto: *zoals op identiteitskaart, zelf genomen of via schoolfotograaf*
- Contact (school): *vast telefoonnummer, e-mailadres v.d. school, gsm-nummer v.d. school*
- Contact (privé): *eigen vast telefoonnummer, eigen e-mailadres, eigen gsm-nummer*
- Loopbaan: *sollicitatie, cv, diploma's, bekwaamheidsbewijzen, opdrachten, verlofstelsels*
- Loon: *barema, anciënniteit, personen ten laste*
- Afwezigheden: *afwezige dagen, redenen, bewijzen*
- Evaluatie: *functioneringsgesprekken, evaluatiegesprekken*
- Levensbeschouwing: *indien (gedeeltelijk) leerkracht Godsdienst*

### 1.3.4 Oud-leerlingen

- Rijksregister: *rijksregisternummer*
- Identificatie: *voornaam, naam, geboortedatum, geboorteplaats en/of identiteitskaartnummer*
- Contact (privé): *eigen vast telefoonnummer, eigen e-mailadres, eigen gsm-nummer*
- Schoolloopbaan: *instellingen, jaren, richtingen, klassen*
- Evaluatie: *deliberaties, verslagen, eindbeslissingen, motiveringen*

### 1.3.5 Oud-personeel

- Rijksregister: *rijksregisternummer*
- Identificatie: *voornaam, naam, geboortedatum, geboorteplaats en/of identiteitskaartnummer*
- Contact (privé): *eigen vast telefoonnummer, eigen e-mailadres, eigen gsm-nummer*
- Loopbaan: *sollicitatie, cv, diploma's, bekwaamheidsbewijzen, opdrachten, anciënniteit*
- Evaluatie: *functioneringsgesprekken, evaluatiegesprekken*

Naast bovenstaande categorieën worden ook nog een beperkt aantal gegevens verwerkt van vrijwilligers, stagiairs en derden.

## 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.**

<b>Niveau 1:</b> Beschikbaarheid is niet nodig	<b>Niveau 2:</b> Beschikbaarheid is onbelangrijk	<b>Niveau 3:</b> Beschikbaarheid is belangrijk	<b>Niveau 4:</b> Beschikbaarheid is noodzakelijk
<i>Het systeem of de informatie is niet (meer) nodig voor de werking van de instelling.</i>	<i>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.</i>	<i>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.</i>	<i>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.</i>
Tussen 0 en 2	Tussen 3 en 7	Tussen 8 en 12	Tussen 13 en 15

### 2.2 Beschikbaarheidsschema

Dit schema wordt ingevuld voor toepassingen waarbij men binnen Dominiek Savio Onderwijs de noodzaak voelt om de beschikbaarheid grondiger dan enkel mondeling te analyseren.

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). *0 staat voor "niet van toepassing"*.

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

### 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.**

<b>Niveau 1:</b> Integriteit is niet noodzakelijk.	<b>Niveau 2:</b> Integriteit is noodzakelijk.	<b>Niveau 3:</b> Integriteit is vereist.	<b>Niveau 4:</b> Integriteit is absoluut.
<i>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.</i>	<i>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.</i>	<i>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.</i>	<i>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.</i>
Tussen 0 en 2	Tussen 3 en 7	Tussen 8 en 13	Tussen 14 en 18

### 3.2 Integriteitsschema

Dit schema wordt ingevuld voor toepassingen waarbij men binnen Dominiek Savio Onderwijs de noodzaak voelt om de integriteit grondiger dan enkel mondeling te analyseren.

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). *0 staat voor "niet van toepassing"*.

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

## 4 Vertrouwelijkheid

### 4.1 Omschrijving

Hiermee wordt de mate bedoeld waarin 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 het dossier van een leerling uit zijn klas te zien, maar niet het dossier van een leerling uit een andere klas. Enkel de leerbegeleiders en de directie zien de dossiers van alle leerlingen.*
- **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.**

<b>Niveau 1:</b> Informatie is openbaar	<b>Niveau 2:</b> Informatie is intern	<b>Niveau 3:</b> Informatie is vertrouwelijk.	<b>Niveau 4:</b> Informatie is geheim.
<i>Openbaar worden van gegevens leidt tot weinig of geen schade voor een instelling of betrokkene.</i>	<i>De organisatie, instelling of betrokkene kan niet meteen aanzienlijke 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 basis).</i>	<i>De organisatie, instelling of betrokkene kan aanzienlijke 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 basis).</i>	<i>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.</i>

## 4.2 Vertrouwelijkheidsschema

Hieronder staat de classificatie van categorieën van persoonsgegevens, zoals ze op Dominiek Savio Onderwijs gehanteerd wordt.

Categorie van persoonsgegevens	Openbaar	Intern	Vertrouwelijk	Geheim	Motivatie
<b>Gegevens van leerlingen</b>					
Rijksregister			x		<i>De instelling is gemachtigd om het rijksregisternummer te verwerken, maar ze mag het niet extern ter beschikking stellen.</i>
Identificatie		x			<i>De instelling heeft deze informatie nodig, maar ze mag het niet extern ter beschikking stellen.</i>
Indicatoren			x		<i>De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.</i>
Pasfoto		x			<i>De instelling heeft deze informatie nodig, maar ze mag het niet extern ter beschikking stellen.</i>
Contact (school)	x				<i>Schoolcontactcoördinatoren mogen extern gebruikt worden.</i>
Contact (privé)			x		<i>Privé contactcoördinatoren mogen niet extern gebruikt worden.</i>
Schoolloopbaan		x			<i>De instelling heeft deze informatie nodig, maar ze mag het niet zomaar extern ter beschikking stellen.</i>
Afwezigheden			x		<i>De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.</i>
Evaluatie (puntenboeken, rapporten)			x		<i>De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.</i>
Evaluatie (deliberaties, verslagen)			x		<i>De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.</i>
Functioneren			x		<i>De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.</i>
Medische informatie				x	<i>De instelling heeft deze gevoelige informatie nodig, maar ze dient deze zorgvuldig af te scherm.</i>



Categorie van persoonsgegevens	Openbaar	Intern	Vertrouwelijk	Geheim	Motivatie
<b>Gegevens van ouder(s) / voogd</b>					
Identificatie		x			De instelling heeft deze informatie nodig, maar ze mag het niet extern ter beschikking stellen.
Adres		x			De instelling heeft deze informatie nodig, maar ze mag het niet extern ter beschikking stellen.
Contact (privé)			x		Privé contactcoördinaten mogen niet extern gebruikt worden.
Financieel: gegevens bank(rekening)			x		De instelling heeft deze informatie nodig, maar ze mag het niet extern ter beschikking stellen.
Financieel: openstaande schuld				x	De instelling heeft deze gevoelige informatie nodig, maar ze dient deze zorgvuldig af te schermen.
Categorie van persoonsgegevens	Openbaar	Intern	Vertrouwelijk	Geheim	Motivatie
<b>Gegevens van personeelsleden</b>					
Rijksregister			x		De instelling is gemachtigd om het rijksregisternummer te verwerken, maar ze mag het niet extern ter beschikking stellen.
Identificatie		x			De instelling heeft deze informatie nodig, maar ze mag het niet extern ter beschikking stellen.
Pasfoto		x			De instelling heeft deze informatie nodig, maar ze mag het niet zomaar extern ter beschikking stellen.
Contact (school)	x				Schoolcontactcoördinaten mogen extern gebruikt worden.
Contact (privé)			x		Privé contactcoördinaten mogen niet extern gebruikt worden.
Loopbaan		x			De instelling heeft deze informatie nodig, maar ze mag het niet zomaar extern ter beschikking stellen.
Afwezigheden			x		De instelling heeft deze informatie nodig, maar niet iedereen dient erover te beschikken.

Financieel: gegevens bank(rekening)			x		<i>De instelling heeft deze informatie nodig, maar ze mag het niet extern ter beschikking stellen.</i>
Financieel: openstaande schuld				x	<i>De instelling heeft deze gevoelige informatie nodig, maar ze dient deze zorgvuldig af te scherm.</i>
Functioneren en evaluatie				x	<i>De instelling heeft deze gevoelige informatie nodig, maar ze dient deze zorgvuldig af te scherm.</i>
Levensbeschouwing				x	<i>De instelling heeft deze gevoelige informatie nodig, maar ze dient deze zorgvuldig af te scherm.</i>
<b>Categorie van persoonsgegevens</b>	<b>Openbaar</b>	<b>Intern</b>	<b>Vertrouwelijk</b>	<b>Geheim</b>	<b>Motivatie</b>
<b>Gegevens van oud-leerlingen</b>					
Rijksregister			x		<i>De instelling is gemachtigd om het rijksregisternummer te verwerken, maar ze mag het niet extern ter beschikking stellen.</i>
Identificatie		x			<i>De instelling heeft deze informatie nodig, maar ze mag het niet extern ter beschikking stellen.</i>
Contact (privé)			x		<i>Privé contactcoördinaten mogen niet extern gebruikt worden.</i>
Schoolloopbaan			x		<i>De instelling heeft deze informatie nodig, maar niet iedereen dient er toegang toe te hebben.</i>
Evaluatie (deliberaties, verslagen)			x		<i>De instelling dient deze informatie bij te houden, maar niet iedereen dient er toegang toe te hebben.</i>
<b>Categorie van persoonsgegevens</b>	<b>Openbaar</b>	<b>Intern</b>	<b>Vertrouwelijk</b>	<b>Geheim</b>	<b>Motivatie</b>
<b>Gegevens van oud-personeelsleden</b>					
Rijksregister			x		<i>De instelling is gemachtigd om het rijksregisternummer te verwerken, maar ze mag het niet extern ter beschikking stellen.</i>
Identificatie		x			<i>De instelling heeft deze informatie nodig, maar ze mag het niet extern ter beschikking stellen.</i>

Contact (privé)			x		<i>Privé contactcoördinaten mogen niet extern gebruikt worden.</i>
Loopbaan			x		<i>De instelling heeft deze informatie nodig, maar niet iedereen dient er toegang toe te hebben.</i>
Functioneren en evaluatie				x	<i>De instelling mag deze gevoelige informatie bijhouden, maar ze dient deze zorgvuldig af te schermen.</i>

# TOEGANGSMATRICES



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

VOOR:

**Basisonderwijs Dominiek Savio** (instellingsnummer 26741)

**Secundair Onderwijs Dominiek Savio** (instellingsnummer 28134)

Versie	Datum	Status	Opmerking
1.0	30/05/2018	ONTWERP	Besproken met CIV op 20/03/2018 en 27/04/2018
1.1	05/06/2018	GOEDGEKEURD	Goedgekeurd door Raad van Bestuur

## 1 Inleiding

### 1.1 Situering

In deze nota bepalen we het gebruikersrechtenbeleid op Dominiek Savio Onderwijs, gebaseerd op de **classificatie van (persoons)gegevens**. Hiermee bedoelen we dat hier omschreven wordt welke gebruikers(groepen) welke toegang 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 maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB) en valt onder de eindverantwoordelijkheid van Dominiek Savio vzw.

### 1.2 Gebruikersgroepen

Alle dragers, platformen, systemen en het netwerk die binnen Dominiek Savio Onderwijs 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:

- *Beheerders (bv. ICT-coördinatoren)*
- *CLB-medewerkers*
- *Directieleden*
- *Leerbegeleiders*
- *Paramedici (opvoeders, verpleging en therapeuten)*
- *Leerkrachten en ondersteuners*
  - *Die lid zijn van de klassenraad (KR) of het klasteam (KT) van de betrokken leerling of deze leerling ondersteunen (OT)*
  - *Die geen lid zijn van de klassenraad of het klasteam van de betrokken leerling of deze leerling niet ondersteunen*
- *Regioverantwoordelijken*
- *Ondersteunend personeel<sup>1</sup>*
- *Ouder(s) of voogd, stiefouder(s)*
- *Betrokkene zelf (desgevallend de ouder(s) of de voogd)*
- *Derden (bv. vrijwilligers, stagiairs, busbegeleiders, externe betrokkenen<sup>2</sup>)*

---

<sup>1</sup> Er wordt naar gestreefd om, indien praktisch haalbaar, de toegang tot gegevens zo veel mogelijk gericht in te stellen naar de specifieke taken en bevoegdheden van elke secretariaatsmedewerker toe (bv. personeelsadministratie, leerlingadministratie, boekhouding, ...).

<sup>2</sup> Hiertoe behoren bv. de medewerkers van externe verwerkers, die in opdracht van Onderwijs Dominiek Savio persoonsgegevens ontvangen en/of verwerken.

Deze groepen worden globaal gehanteerd binnen het IVP-beleid van Dominiek Savio Onderwijs. Mogelijks bestaan er, voor welbepaalde gevallen of toepassingen, hiernaast nog specifiekere gebruikers- en beveiligingsgroepen.

Naast onderstaande toegangsmatrices wordt er per toepassing ook een concreet en gedetailleerd overzicht bijgehouden van personeelsleden / gebruikersgroepen en hun toegangsrechten.

### 1.3 Gebruikersrechten

De algemeen gehanteerde gebruikersrechten zijn:

- GT: geen toegang (*men kan de gegevens niet opvragen of zien. Ze worden ook niet in overzichten of dergelijke vermeld*);
- L: leesttoegang (*men kan alles zien, maar niets verwijderen, toevoegen of aanpassen*);
- W: wijzig- of schrijftoegang (*men kan alles zien, items toevoegen en aanpassen, op sommige platformen is het mogelijk om apart 'verwijderrechten' al dan niet toe te kennen, maar in dit document wordt dit samen gerekend met het wijzigrecht*)<sup>3</sup>
- VB: volledig beheer (*dit wil zeggen dat men ook de toegangsrechten, van zichzelf en van anderen, kan aanpassen*).

## 2 Toegangsmatrices

Voor de oplijsting van de concrete gegevens die zich in de hier gehanteerde vertrouwelijkheidsniveaus 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 Persoonsgegevens van leerlingen

	Beheerders	CLB-medewerkers	Directieleden	Leerbegeleiders	Paramedici	Leerkrachten/ondersteuners (KR,KT,OT)	Leerkrachten/ondersteuners (geen KR, KT, OT)	Regioverantwoordelijken	Ondersteunend personeel (bevoegd)	Ouder(s), voogd	Betrokkene zelf	Derden, externen
Openbaar	VB	L	L						GT	L	GT	
Intern			W	L			W		GT			
Vertrouwelijk				L of W		GT	W					
Geheim				L of W	GT of L		W	GT of L				

<sup>3</sup> Mogelijks zijn deze rechten enkel van toepassing op items die door de persoon zelf toegevoegd werden (eigenaarschap) en niet noodzakelijk ook op items van andere gebruikers. Een versiebeheer houdt bij wie wanneer welke aanpassingen aan de inhoud doet.

Noten; toelichting:

- Ouder(s), voogden en betrokkenen zelf: hebben recht op informatie, inzage en correctie. Dit wil niet zeggen dat ze automatisch toegang tot het leerlingvolg- of leerlingevaluatiesystemen moeten krijgen.
- De klassendirecteurs, de regio-verantwoordelijken en de paramedici krijgen desgevallend wijzigrechten op alle leerlinggegevens van hun klassenraad/team, teneinde verslaggeving en administratieve opvolging op te nemen.

## 2.2 Persoonsgegevens van ouder(s), stiefouder(s) of voogd(en)

	Beheerders	CLB-medewerkers	Directieleden	Leerbegeleiders	Paramedici	Leerkrachten/ondersteuners (KR,KT,OT)	Leerkrachten/ondersteuners (geen KR, KT, OT)	Regioverantwoordelijken	Ondersteunend personeel (bevoegd)	Ouder(s), voogd	Betrokkene zelf	Derden, externen
Openbaar	niet van toepassing											
Intern	VB	L	W	W	L	L	GT	W	W	GT	GT	GT
Vertrouwelijk												
Geheim	niet van toepassing											

Specifieke rechten; uitzonderingen:

Financiële gegevens	VB	GT	W	GT	GT	GT	GT	GT	W	GT	GT	GT
---------------------	----	----	---	----	----	----	----	----	---	----	----	----

Noten; toelichting:

- Financiële gegevens: openstaande rekeningen en afbetalingen mogen enkel maar door een beperkt aantal bevoegde personen verwerkt 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.

## 2.3 Persoonsgegevens van personeelsleden

	Beheerders	CLB-medewerkers	Directieleden	Leerbegeleiders	Paramedici	Leerkrachten/ondersteuners (KR,KT,OT)	Leerkrachten/ondersteuners (geen KR, KT, OT)	Regioverantwoordelijken	Ondersteunend personeel (bevoegd)	Ouder(s), voogd	Betrokkene zelf	Derden, externen
Openbaar	VB	L	W	L				L of W	W	L		
Intern		GT		L						GT of W	GT of L	GT
Vertrouwelijk				GT								
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 moet krijgen, behoudens de openbare gegevens.

## 2.4 Gegevens van oud-leerlingen

	Beheerders	CLB-medewerkers	Directieleden	Leerbegeleiders	Paramedici	Leerkrachten/ondersteuners (KR,KT,bgl)	Leerkrachten/ondersteuners (geen KR, KT, bgl)	Regioverantwoordelijken	Ondersteunend personeel (bevoegd)	Ouder(s), voogd	Betrokkene zelf	Derden, externen
Openbaar	niet van toepassing											
Intern	VB	GT	W	GT				W	GT			
Vertrouwelijk	niet van toepassing (verwijderd)											
Geheim	niet van toepassing (verwijderd)											

Specifieke rechten; uitzonderingen:

Rijksregister-nummer	VB	GT	L	GT	GT	GT	GT	L	L	GT	GT	GT
----------------------	----	----	---	----	----	----	----	---	---	----	----	----



Noten; toelichting:

- Bij interne gegevens rekenen we in dit geval de leerlinggebonden documenten waarvoor een wettelijke bewaartermijn geldt, zoals identificatiegegevens (uitgezonderd rijksregisternummer), contactgegevens, deliberatiebeslissingen, notulen van de klassenraad, enz.
- 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.

## 2.5 Gegevens van oud-personeelsleden

	Beheerders	CLB-medewerkers	Directieleden	Leerbegeleiders	Paramedici	Leerkrachten/ondersteuners (KR,KT,bgl)	Leerkrachten/ondersteuners (geen KR, KT, bgl)	Regioverantwoordelijken	Ondersteunend personeel (bevoegd)	Ouder(s), voogd	Betrokkene zelf	Derden, externen
Openbaar	niet van toepassing											
Intern	niet van toepassing											
Vertrouwelijk	VB	GT	W	GT					W	GT		
Geheim	(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 moet krijgen.

## 3 Vergrendelingsbeleid

### 3.1 Wat is een vergrendelingsbeleid

Toegangsbeperkingen hebben weinig zin indien er geen beleid is rond de (“geldigheidsduur” van de) gehanteerde gebruikersaccount zelf. Dit beleid maakt, samen met het **wachtwoordbeleid**, deel uit van wat men IAM (*Identity & Access Management*) noemt.



### 3.2 Bepalingen

- Elk gebruikersaccount behoort toe aan één uniek individu. Er worden op Dominiek Savio Onderwijs geen accounts gedeeld gebruikt en er worden geen anonieme accounts gebruikt.
  - ➔ Uitzondering hierop zijn de klasaccounts die gebruikt worden door alle leerlingen van 1 klas in het basisonderwijs.
- Indien men een aantal maal (aantal afhankelijk van de toepassing) probeert aan te melden met een foutief wachtwoord, dan wordt de gebruikersaccount vergrendeld. Men kan de beheerder(s) contacteren om de account te ontgrendelen, desgevallend met een gereset wachtwoord (zie ook het **wachtwoordbeleid** § 3.5).
- Gebruikersaccounts van personeelsleden die uit dienst treden resp. van leerlingen die de school verlaten, worden uitgeschakeld maximum 2 weken na uitdiensttreding resp. vertrek.
- Personeelsleden die het einde van hun aanstelling van bepaalde duur bereiken, verliezen maximum twee weken volgend op het einde van de overeenkomst hun aanmeldrechten.
- Leerlingen die afstuderen, behouden hun aanmeldrechten tot en met 1 juli van het jaar dat ze afstuderen. Daarna hebben ze geen toegang meer tot de platformen. Het behoort tot de pedagogische opdracht van de school om leerlingen aan te leren een persoonlijke e-mail aan te maken en een back-up te maken van de gegevens die ze nog wensen te bewaren uit hun schoolaccount.
- Gebruikersaccounts van personeelsleden die Dominiek Savio Onderwijs verlaten omwille van een tijdelijke tewerkstelling buiten onze school, worden vergrendeld gedurende de ganse periode van hun afwezigheid. Desgevallend behouden zij de toegang tot uitsluitend het interne communicatiesysteem.

# WACHTWOORDBELEID



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

VOOR:

**Basisonderwijs Dominiek Savio** (instellingsnummer 26741)

**Secundair Onderwijs Dominiek Savio** (instellingsnummer 28134)

Versie	Datum	Status	Opmerking
1.0	30/05/2018	ONTWERP	Besproken met Hannes Rondelez en Greg Messiaen op 19/03/2018 Besproken met Peter Messeyne op 19/04/2018 Besproken met CIV op 27/04/2018
1.1	05/06/2018	GOEDGEKEURD	Goedgekeurd door Raad van Bestuur

## 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**, **autorisatie** en **auditing**.

**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: enkel personeelsleden die lid zijn van de klassenraad kunnen het dossier van een leerling van die klas lezen. Leerkrachten die niet met die leerling werken, hebben geen toegang tot dat dossier.

**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 Dominiek Savio Onderwijs.

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB) en valt onder de eindverantwoordelijkheid van Dominiek Savio vzw.

## 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 Authenticeren

Er zijn verschillende manieren om je in systemen te authenticeren. 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 authenticeren. 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 Dominiek Savio Onderwijs werken we er 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 8 karakters hebben.
- Beter nog is om te werken met een wachtwoordzin (bijv: IkGaSinds2015NaarDeSchool)
- Mix hoofdletters, kleine letters en tekens door elkaar: gebruik volgende tekens 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.
- Verander minstens één keer per schooljaar je wachtwoord voor de verschillende onderwijstoepassingen.
- Gebruikersaccounts schooltoestellen:
  - Voor personeel: het wachtwoord dient om de drie maanden gewijzigd te worden door het personeel. Wachtwoorden worden nergens bijgehouden. Wachtwoorden worden bezorgd via e-mail, maar dienen gewijzigd te worden bij eerste maal inloggen.
  - Voor leerlingen: voor bepaalde leerlingengroepen is het intypen, laat staan bedenken en onthouden van een wachtwoord niet evident. Daarom wordt er elk jaar een nieuw, veilig wachtwoord ingesteld door de ICT-coördinatoren. De wachtwoorden dienen niet gewijzigd te worden bij de eerste maal inloggen.
- Gebruik verschillende wachtwoorden voor verschillende applicaties; hergebruik je wachtwoord niet!

Gebruik een online tool om te zien hoe sterk jouw wachtwoord is: bijv. <https://veiliginternetten.nl/wachtwoord-check>

### 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.
- Verzend nooit een wachtwoord via e-mail of een ander communicatiesysteem. Niemand van Dominiek Savio Onderwijs zal ooit je wachtwoord, om eender welke reden, op deze manier opvragen.
- Bij uitzondering kan het nodig zijn dat de ICT-coördinator je wachtwoord nodig heeft om een probleem aan de computer te verhelpen. Indien gewenst, kan je je wachtwoord nadien wijzigen.
- De ICT-coördinator kan je wachtwoord(en) via e-mail bezorgen. In de meeste gevallen moet je je wachtwoord wijzigen na de eerste keer inloggen (uitgezonderd leerlingen). Indien je het wachtwoord niet wijzigt, is het aangeraden je wachtwoord uit het hoofd te leren of ergens op een veilige plaats bewaren en nadien deze e-mail te verwijderen.
- 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. NaamAchternaamGeboortjaar, 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

- Mogelijks wordt je account na een aantal pogingen om in te loggen (afhankelijk van de toepassing), vergrendeld. Neem contact op met de ICT-coördinator om het account terug te ontgrendelen.
- Laat de computer nooit onbeheerd achter maar vergrendel het scherm (Win + L) of log uit.
- Er wordt automatisch gecontroleerd op het gebruik van goede wachtwoorden.
- Als je je schoolaccount gebruikt op een eigen (mobiel) toestel, stel dan zeker ook een vergrendeling (toegangscode, wachtwoord, vingerafdruk, ...) in op dat toestel.

### 3.4 Wat doen bij vermoeden van misbruik?

Misbruik kan ontvreemding of onrechtmatig gebruik van een wachtwoord zijn.

- Verander het wachtwoord onmiddellijk (of laat het veranderen door de ICT-coördinator)

- Neem direct contact op met het aanspreekpunt informatieveiligheid of de ICT-coördinator. Meldpunt datalekken: [privacy@dominieksavio.be](mailto:privacy@dominieksavio.be)

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

### 3.5 Wat doen indien het wachtwoord vergeten werd

- Blijf niet proberen; na een aantal pogingen zal je account vergrendeld worden (zie § 3.3)
- 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 “back-up” e-mailadres, waarmee men een nieuw wachtwoord kan instellen (zonder het vorige te kennen).
- Anders neem je persoonlijk contact op met de ICT-coördinator. Zij zullen een nieuw wachtwoord instellen (d.i. een “wachtwoordreset”) waarmee de gebruiker terug kan aanmelden.

### 3.6 Gebruik van wachtwoordmanagers of een wachtwoordkluis

Indien je te veel wachtwoorden moet onthouden, kan je gebruik maken van een wachtwoordkluis. Wachtwoordkluisen 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 ontsleutelen.

De volgende wachtwoordkluis wordt aangeraden voor onze school, zal ook verder toegelicht worden tijdens bijscholingen en kan je voor ondersteuning terecht bij de ICT-coördinator:

- LastPass (<https://lastpass.com/nl/>)

Deze wachtwoordkluisen werden ook veilig bevonden:

- KeePass (<http://keepass.info/>)
- 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 ontftuseld 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. Binnen Dominiek Savio Onderwijs zullen deze in schooljaar 18-19 uitgetest worden door personen die **op Smartschool** toegang hebben tot **veel, zo niet alle, leerlingendossiers of het volledige Intradesk**, bv. smartschoolbeheerders, directie, leerbegeleiders, regio-verantwoordelijken, ondersteunend personeel.

Indien het systeem van two-factor authentication haalbaar bevonden wordt, kan deze uitgebreid worden naar de rest van het personeel.



## 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 worden en kunnen gegevens gestolen worden.

Rond deze risico's worden alle personeelsleden, maar ook de leerlingen en ouders, binnen Dominiek Savio Onderwijs 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



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

VOOR:

**Basisonderwijs Dominiek Savio** (instellingsnummer 26741)

**Secundair Onderwijs Dominiek Savio** (instellingsnummer 28134)

Versie	Datum	Status	Opmerking
1.0	30/05/2018	ONTWERP	Besproken met Ben Debrouwer, Helder Geeraert, Miet Grymonprez en Evi Formesyn 23/03/2018 Besproken met CIV op 28/05/2018
1.1	05/06/2018	GOEDGEKEURD	Goedgekeurd door Raad van Bestuur

## 1 Inleiding

De manier waarop personeelsleden, en ook leerlingen en ouders, communiceren maakt ook 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 en het imago van Onderwijs Dominiek Savio op een gepast niveau wordt behouden.

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB) en valt onder de eindverantwoordelijkheid van Dominiek Savio vzw.

## 2 Discretieplicht

Alle personeelsleden van Onderwijs Dominiek Savio zijn gebonden aan een **discretieplicht**, ten aanzien van de persoonsgegevens van leerlingen, ouders of het gezin, en ten aanzien van elkaars persoonsgegevens. In het *algemeen reglement van het personeel van het katholiek onderwijs* (art. 7 § 7, art. 23 § 1) wordt hiernaar verwezen.

Dit betekent concreet dat zij van ambtswege uit, geen persoonsinformatie mogen vermelden of publiceren, buiten de daarvoor voorziene kanalen binnen Onderwijs Dominiek Savio. 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 privacyprocedures en -afspraken steeds 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 Onderwijs Dominiek Savio is het meldpunt datalekken: [privacy@dominieksavio.be](mailto:privacy@dominieksavio.be).

## 3 E-mailbeleid

Voor personeelsleden wordt hiernaar verwezen in het arbeidsreglement van Onderwijs Dominiek Savio, Hoofdstuk VI, art. 14-15-16-17 en bijlage 3.

We onderscheiden drie categorieën e-mailadressen:

- Algemene school e-mail (zoals o.a. [info@dominieksavio.be](mailto:info@dominieksavio.be), [second@dominieksavio.be](mailto:second@dominieksavio.be), [ondersteuningsteam.type4@dominieksavio.be](mailto:ondersteuningsteam.type4@dominieksavio.be), ... )
- Privé e-mail (zelf aangemaakte Gmail, Hotmail, Outlook, Live, Yahoo, ... account)
- Persoonlijke school e-mail (van de vorm [voornaamnaam@dominieksavio.be](mailto:voornaamnaam@dominieksavio.be) of [voornaam.naam@dominiek-savio.be](mailto:voornaam.naam@dominiek-savio.be))

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 e-mail of een ander communicatiesysteem. Niemand van Onderwijs Dominiek Savio zal op deze manier ooit een wachtwoord opvragen. Enkel de ICT-coördinator zal u uw paswoord(en) via e-mail bezorgen. In veel gevallen zal u dit paswoord na de eerste keer aanmelden moeten wijzigen.*

### 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 en deze groep bevat (externe) e-mailadressen die zichtbaar gemaakt kunnen worden, dan dient men het steeds in “blind carbon copy” (BCC) te plaatsen.

### 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 Onderwijs Dominiek Savio, 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 bij het gebruik van privé accounts, op toestellen of een netwerk waarop zich ook persoonsgegevens van Onderwijs Dominiek Savio bevinden, op dat bijlagen, hyperlinks, tools, ... die met de privé accounts gebruikt worden, niet leiden tot beveiligingsgevaren zoals virussen, ransomware, phishing<sup>1</sup> enz.

---

<sup>1</sup> 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.

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

- Deze accounts worden aan de medewerker voor professioneel gebruik beschikbaar gesteld. Gebruik is derhalve 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 in de zin van § 3.2 oplevert:
  - 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.
- Het is niet toegestaan dit account te gebruiken voor privé commerciële doeleinden.

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 iedereen privacy en/of de informatieveiligheid als geheel te waarborgen. Mogelijks leidt dit er toe dat Onderwijs Dominiek Savio niet alle rechten en vrijheden van leerlingen, ouders of medewerkers kan waarborgen. Met gevoelige informatie bedoelen we o.a. gezinssituatie, psycho-sociaal, medisch, zorg, financieel.  
Gebruik indien mogelijk het (centraal beheerde en beveiligde) leerlingvolgsysteem om deze informatie met de juiste collega's en medewerkers te delen.
- Indien u via dit e-mailaccount (gevoelige) persoonsgegevens ontvangt, plaats deze dan zo snel mogelijk in het (centraal beheerde en beveiligde) **leerlingvolgsysteem** of laat een bevoegde medewerker dit er in plaatsen.  
Het is wenselijk om daarna alle berichten die deze gegevens bevatten of behandelden te verwijderen (ook uit uw "Prullenmand").
- Gebruik dit account niet op het world wide web, voor platformen die niet nodig zijn om uw taak voor Onderwijs Dominiek Savio uit te voeren of voor platformen **die niet "informatieveilig" beschouwd worden** door het aanspreekpunt informatieveiligheid. Contacteer voor vragen hierrond [privacy@dominieksavio.be](mailto:privacy@dominieksavio.be).
- Maak zo veel mogelijk gebruik van "blind carbon copy" (BCC) indien u met meerdere mensen communiceert, zeker als het om externe e-mailadressen gaat.

- Let op wie u bij de ontvangers plaatst of in kopieert, met “carbon copy” (CC). Weest zuinig op het aantal personen dat u in CC plaatst. Is dat wel nodig?
- Het automatisch doorsturen van e-mails van uw schoolaccount naar uw privé e-mailadres is niet toegestaan.



The screenshot shows an email composition interface with the following fields:

- Nieuw bericht** (Title bar)
- Aan** (To field)
- Cc** (Carbon Copy field)
- Bcc** (Blind Carbon Copy field)
- Van** (From field)
- Onderwerp** (Subject field)

## 4 Beleid inzake communicatie-apps

Naast e-mail, zijn er tegenwoordig tal van andere communicatieplatformen, ook op mobiele toestellen. Op Onderwijs Dominiek Savio 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, i.h.b. ten aanzien van privacygevoelige informatie.

We raden medewerkers, ouders en leerlingen verbonden aan Onderwijs Dominiek Savio aan hoofdzakelijk één of meerdere van de volgende communicatieplatformen te gebruiken:

- Het intern berichtensysteem van GSuite for Education (GMail met voornaamnaam@dominieksavio.be) en voor ondersteunend personeel en directie ook het berichtensysteem van Groep Gidts (Office365 met voornaam.naam@dominiek-savio.be).
- Instant messaging via telefonie: SMS
- Instant messaging online: Google Hangouts, Hangouts Chat
- Video conferencing: Google Hangouts of Meet

### 4.1 Intern berichtensysteem

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

Indien men het interne communicatiesysteem (en eventueel andere functionaliteiten of modules) raadpleegt op een mobiel toestel, vragen wij om dit toestel met een vergrendeling te beveiligen (zie § 5.2 in het **toestelbeleid**).

### 4.2 Instant messaging (SMS of online)

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

Indien deze kanalen en/of school e-mailaccounts 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 toch gebruik gemaakt wordt van stem- of video-opnames, kan dit enkel mits uitdrukkelijke en voorafgaande toestemming van de verschillende partijen.

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

## 5 Social Media-protocol

Bron: <https://www.hetstreek.nl/sites/default/files/Protocol%20Sociale%20Media%20%20-%20april%202012.pdf>

### 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 Onderwijs Dominiek Savio .

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 Onderwijs Dominiek Savio 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.

Onderwijs Dominiek Savio 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. Onderwijs Dominiek Savio 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. Onderwijs Dominiek Savio 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 Onderwijs Dominiek Savio .

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 de schoolleiding, leraren en/of onderwijsondersteunend personeel toestemming is gegeven.
2. Het is medewerkers toegestaan om tijdens de schoolopdracht 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. De betrokkene is persoonlijk verantwoordelijk voor de inhoud welke 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 de sociale media te zetten tenzij de betrokkenen hier uitdrukkelijk (bij voorkeur op papier of digitaal) 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 Onderwijs Dominiek Savio afgeraden om privé pagina's en uitingen te delen die het imago van de school, hun medewerkers en/of leerlingen kunnen schaden. Ook het zogenaamde 'vrienden' worden met leerlingen van Onderwijs Dominiek Savio of aan wie Onderwijs Dominiek Savio ondersteuning biedt, wordt niet toegestaan. De communicatie op deze sociale media vindt plaats via generieke (speciaal voor dit doel aangemaakte) 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/profiel op sociale media wordt aangemaakt, dan wordt hiervoor een generiek, duidelijk aan school gebonden profiel of pagina gebruikt. Het aanmaken hiervan wordt op voorhand met de directeur besproken en de link naar dit profiel of de pagina wordt doorgegeven aan het aanspreekpunt informatieveiligheid. Zo kan de school het overzicht behouden van aan-school-gebonden profielen en pagina's op sociale media.

2. Elke betrokkene is zich bewust van het feit dat (op sommige sociale media) ook anderen informatie kunnen plaatsen op (profiel) pagina's (taggen, linken, posten, etc.).

3. Om die reden zal de eigenaar van de pagina (off-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 op non-actief gesteld.

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



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

VOOR:

**Basisonderwijs Dominiek Savio** (instellingsnummer 26741)

**Secundair Onderwijs Dominiek Savio** (instellingsnummer 28134)

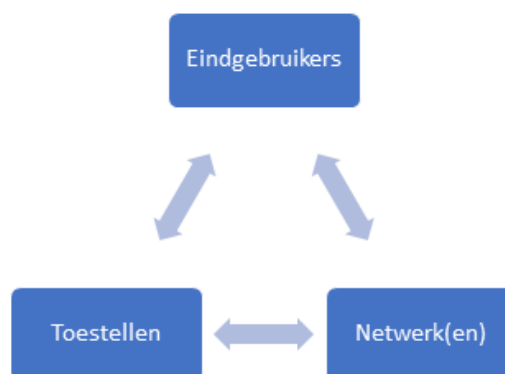
Versie	Datum	Status	Opmerking
1.0	30/05/2018	ONTWERP	Besproken met Hannes Rondelez en Greg Messiaen op 19/03/2018 Besproken met Peter Messeyne op 19/04/2018 Besproken met CIV op 27/04/2018
1.1	05/06/2018	GOEDGEKEURD	Goedgekeurd door Raad van Bestuur

## 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 Dominiek Savio Onderwijs enerzijds regels bepalen om de bijdrage van elk van deze drie aspecten in het IVP-beleid te maximaliseren, en anderzijds wordt toegelicht hoe op Dominiek Savio Onderwijs **controle** op elk van deze aspecten gevoerd wordt.

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB) en valt onder de eindverantwoordelijkheid van Dominiek Savio vzw.

### 1.2 Algemene bepalingen

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

- Het voorzien van manieren om te herkennen wanneer het “gewone” verkeer gemonitord, onderschept, nagebootst of gewijzigd wordt.
- 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 vinden geen ongeoorloofde inzages of systematische analyses 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, hubs, kabels, servers, modems, ...

De algemene maatregelen (zie § 1.2) worden toegepast, met i.h.b. logging van bv. tijdsregistratie, MAC- en IP-adressen, toestelnamen, gebruikersnamen.

Wachtwoorden op de netwerkcomponenten worden systematisch gewijzigd t.o.v. de “default” waarden, of te gemakkelijke combinaties. De gekozen wachtwoorden voldoen i.h.b. aan alle afspraken uit het **wachtwoordbeleid**.

## 2.2 Wifi-netwerk

Voor personeel, leerlingen en gasten is wifi voorzien op Dominiek Savio Onderwijs. Deze dienst is gratis voor de eindgebruikers, maar heeft voor de school wel een zekere kostprijs (in aanschaf, onderhoud en beveiliging).

Daarom wordt de aard en hoeveelheid van het netwerkverkeer gemonitord.

De algemene maatregelen (zie § 1.2) worden toegepast, met i.h.b. logging van bv. tijdsregistratie, MAC- en IP-adressen, toestelnamen, gebruikersnamen.

Ook de gebruikte applicaties en het datagebruik via het draadloze netwerk, wordt bijgehouden in logboeken en kan desgevallend wel geanalyseerd worden, als het globale verbruik dit rechtvaardigt. Alle informatie hier aangaande wordt strikt vertrouwelijk behandeld.

Het netwerkverkeer dat via het draadloze netwerk verloopt, wordt versleuteld. Het raadplegen, bewerken enz. van persoonsgegevens kan dus ook veilig gebeuren via het draadloze netwerk.

## 3 Beveiliging en controle op internetverkeer

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

Als organisatie is Dominiek Savio Onderwijs verantwoordelijk voor het algehele dataverbruik, en voor alles dat er met / via deze internetverbinding gebeurt. Daarom hanteert men ook hier een aantal regels en controles daarop:

De algemene maatregelen (zie § 1.2) worden toegepast, met i.h.b. logging van bv. tijdsregistratie, MAC- en IP-adressen, toestelnamen.

## 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.

## 4.1 Algemeen

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

- Het internetverkeer en de gebruikte toepassingen worden, op verscheidene niveaus, gecontroleerd inzake bv. bezochte doelsites, uitgaand verkeer, capaciteit, maar ook veiligheid van de toepassing.
- Afdrukopdrachten worden geregistreerd: toestelnaam, printernaam, gebruikersnaam, documentnaam, datum, tijd, aantal pagina's.
- 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 Dominiek Savio Onderwijs dan ook verschillende maatregelen genomen om dit te verhinderen. Het doelbewust veranderen van systeem- of beveiligingsinstellingen is verboden.

Dit beleid wordt 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, met bv. logging van tijdsregistratie, MAC- en IP-adressen, gebruikersnamen, toestelnamen, logintijd, wijzigingen in systeeminstellingen.

- Op Dominiek Savio Onderwijs worden er bepaalde tools gebruikt die het mogelijk maken de actieve vensters en/of het real-time beeldscherm van de schooltoestellen over te nemen.
  - Momenteel worden deze tools enkel gebruikt door de ICT-coördinatoren voor onderhoud van de toestellen, ondersteuning of probleemoplossing van op afstand.
  - Indien het toestel in gebruik is tijdens de schooluren, vragen ICT-coördinatoren steeds vooraf toestemming (bv. via de chatfunctie) om het beeldscherm vanop afstand over te nemen.
  - Indien het toestel niet in gebruik is tijdens de schooluren, kan het vanop afstand aangezet, overgenomen en weer uitgezet worden door de ICT-coördinatoren.
  - Voor en na de schooluren, als er in principe niemand meer in het schoolgebouw aanwezig is, kunnen toestellen ongevraagd overgenomen worden of worden toestellen die uitstaan vanop afstand aangezet (Wake On Lan) of omgekeerd, worden toestellen die nog aanstaan, vanop afstand uitgezet.
  - Voor laptops die toegewezen zijn aan één persoon (bv. directie, ondersteunend personeel) wordt altijd toestemming gevraagd, aangezien deze ook buiten de schooluren gebruikt worden.
- In de toekomst worden tools voor schermovername of monitoring mogelijks ook gebruikt door andere personeelsleden binnen de klascontext. De doeleinden hiervan zijn dan louter en alleen pedagogisch. Het is i.h.b. leerkrachten en ondersteunend personeel *niet* toegestaan om zonder concreet vermoeden van doelbewuste en ernstige inbreuken en zonder overleg met de directie, schermafdrucken te bewaren, een scherm op te nemen of een scherm over te nemen zonder toestemming van de betrokkene.
- Personeelsleden zullen dan, in het kader van hun uit te oefenen taak, de actieve vensters, geopende websites en/of het beeldscherm van de leerlingen kunnen 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 beheerders, directie en eventueel andere personeelsleden die hiervoor bevoegd geacht worden, de schermen bewaren (als een schermafdruck 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 schermafdrucken of opnames.

## 4.2 Vergrendeling, encryptie en wissen van op afstand

De mobiele toestellen (d.w.z. laptops, pda's, tablets, smartphones) die bepaalde personeelsleden gebruiken maar die eigendom zijn van Dominiek Savio Onderwijs, dienen extra beveiligd te worden indien er persoonsgegevens op bewaard, bekeken of verwerkt worden.

I.h.b. wordt er een vergrendeling a.d.h.v. wachtwoord, pincode, swipe code, vingerafdruk of andere authenticatie toegepast.

Voor tablets, smartphones en sommige laptops geldt bovendien:

- Optie om het toestel te lokaliseren of te wissen van op afstand, in geval van diefstal of verlies

## 5 Beveiliging en controle op toestellen van eindgebruikers zelf

Op Dominiek Savio Onderwijs is het mogelijk om met eigen toestellen gebruik te maken van het draadloos netwerk van de school (zie ook § 2). Het is de bedoeling dat dit draadloze netwerk gebruikt wordt 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. Desalniettemin gelden alle principes van deze paragraaf evenzeer voor handelingen gerelateerd aan Dominiek Savio Onderwijs, 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<sup>1</sup>-beleid, zijn:

Het internetverkeer en gebruikte toepassingen wordt, op verscheidene niveaus, gecontroleerd inzake bv. bezochte doelsites, uitgaand verkeer, capaciteit, maar ook veiligheid van de toepassing.

De algemene maatregelen (zie § 1.2) worden toegepast, met bv. logging van: MAC- en IP-adressen, toestelnamen, logintijd, enz.

---

<sup>1</sup> BYOD = "bring your own device". Het gebruik van eigen toestellen op en voor school gerelateerde processen.

## 5.2 Vergrendeling, encryptie, antivirusbeveiliging, back-ups en wissen van op afstand

De mobiele toestellen (d.w.z. laptops, tablets, smartphones) van medewerkers, waarop persoonsgegevens van Dominiek Savio Onderwijs 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 en bij de meeste toestellen afgedwongen via mobiel apparaatbeheer.
- Bij smartphones en tablets waarop een schoolaccount gebruikt wordt, kan deze account bij diefstal of verlies in de meeste gevallen gewist worden. Bij oudere toestellen kan het hele toestel gewist worden.
- Er wordt gevraagd om ten allen tijde een up-to-date antivirusprogramma te gebruiken.
- Back-ups dienen genomen, bewaard en beheerd te worden zoals in het respectievelijke beleid vastgelegd.

## 6 Gebruik van verwisselbare media

Onder verwisselbare media wordt verstaan: usb-sticks, externe harde schijven, cd's, dvd's, ...

Het gebruik van verwisselbare media voor het opslaan van **(gevoelige) persoonsgegevens** wordt **afgeraden** op Dominiek Savio Onderwijs. In de plaats raden we aan om gebruik te maken van de door de school aangeboden opslagruimte in Google Drive for Education, op de server of op Smartschool.

Als een personeelslid **geen andere mogelijkheid** heeft (bv. bij het ontbreken van een internetverbinding), kan verwisselbare media gebruikt worden om (gevoelige) persoonsgegevens op te slaan. In dit geval is het personeelslid **verplicht** om:

- vanaf 01/01/2019 de verwisselbare media te **versleutelen** (het versleutelen van de inhoud op bv. een USB-stick zorgt ervoor dat iemand die de USB-stick vindt of steelt, de gegevens niet kan raadplegen of verspreiden).
- steeds te zorgen voor een **actuele back-up** van de persoonsgegevens op de verwisselbare media op minstens één andere veilige locatie.
- Bij het wegdoen van de verwisselbare media dient men ervoor te zorgen dat de verwisselbare media grondig gewist (met speciale software) of vernietigd wordt.

Personeel kan steeds terecht bij de ICT-coördinatoren voor ondersteuning bij het versleutelen, back-uppen of wissen van verwisselbare media. Er zullen hierover ook bijscholingen worden voorzien.

Zie ook procedure rond gebruik van verwisselbare media.

## 7 Opslaan in 'de cloud'

Indien (gevoelige) persoonsgegevens opgeslaan worden 'in de cloud', wordt er gevraagd om dit enkel te doen in de cloudvoorzieningen die door de school aangeboden worden, nl. Google Drive horende bij G Suite for Education en Smartschool (bv. Mijn Documenten).

Het in de cloud opslaan van (gevoelige) persoonsgegevens bij andere clouddiensten waaronder bv. Google Drive voor particulieren, One Drive, iCloud, Dropbox, Box, Stack, Mega, ... is niet toegestaan.

Enkel indien de voorzieningen van de school geen afdoende oplossing bieden, kan in overleg met directie, ICT-coördinatoren en het AIV, een andere clouddienst gebruikt worden, bv. kan de directie wel gebruik maken van Dropbox, in het belang van samenwerking met Groep Gidts.

# BACK-UPBELEID



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

VOOR:

**Basisonderwijs Dominiek Savio** (instellingsnummer 26741)

**Secundair Onderwijs Dominiek Savio** (instellingsnummer 28134)

Versie	Datum	Status	Opmerking
1.0	30/05/2018	ONTWERP	Besproken met Hannes Rondelez en Greg Messiaen op 19/03/2018 Besproken met Peter Messeyne op 19/04/2018 Besproken met CIV op 27/04/2018
1.1	05/06/2018	GOEDGEKEURD	Goedgekeurd door Raad van Bestuur



# 1 Inleiding

## 1.1 Situering

Voor de gegevens die een bepaald niveau van beschikbaarheid en/of integriteit vereisen, is een goed uitgestippeld back-upbeleid 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-niveaus.

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB) en valt onder de eindverantwoordelijkheid van Dominiek Savio vzw.

### Enkele begrippen

UPS ( <i>uninterrupted power supply</i> ) Noodstroomvoorziening	<i>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 kunnen weggeschreven worden voordat het systeem afgesloten wordt.</i>
Redundantie	<i>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.</i>
Back-ups	<i>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 back-ups wordt bepaald door de classificatie van de gegevens in kwestie. Dit proces kan volledig geautomatiseerd gebeuren.</i>
Synchronisatie	<i>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.</i>

## 2 Stroomvoorziening

De servers waarop gegevens gebruikt of bewaard worden die behoren tot het beschikbaarheidsniveau **noodzakelijk** en/of het integriteitsniveau **absoluut**, worden in Dominiek Savio Onderwijs voorzien van een redundante noodstroomvoorziening.

Gegevens die behoren tot het beschikbaarheidsniveau **belangrijk** en/of het integriteitsniveau **vereist**, worden voorzien van een (gewone) 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 Dominiek Savio Onderwijs voorzien van een alternatieve internetverbinding, met een vergelijkbare bandbreedte en performantie.

Indien mogelijk, worden voor deze systemen SLA's (=Service Level Agreement) afgesloten met de ISP('s) (=Internet Service Provider) in kwestie.

### 4 Back-ups

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

Gegevens die behoren tot het beschikbaarheidsniveau **noodzakelijk** en/of het integriteitsniveau **absoluut**, worden simultaan gesynchroniseerd op minstens één geografisch gespreide locatie.

Alle andere gegevens worden minstens één keer per week geback-upt.

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

Alle back-ups worden conform de gangbare "best practices" bewaard.

**Personeelsleden die persoonsgegevens bewaren op eigen toestellen of in hun Google Drive verbonden aan G Suite for Education, dienen steeds zelf te zorgen voor een actuele back-up van deze gegevens op minstens één veilige locatie.**

### 5 Brandveiligheid

De plaatsen op Dominiek Savio Onderwijs waar gegevens bewaard worden die behoren tot het beschikbaarheidsniveau **belangrijk** en/of het integriteitsniveau **vereist**, of hoger, worden voorzien van afdoende brandbeveiligingsmaatregelen.

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

# IVPB

## ACHTERGRONDINFORMATIE



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

voor:

**Basisonderwijs Dominiek Savio** (inst. nr. 26741)

**Secundair Onderwijs Dominiek Savio** (inst. nr. 28134)

Versie	Datum	Status	Opmerking
1.0	30/05/2018	ONTWERP	
1.1	05/06/2018	GOEDGEKEURD	Goedgekeurd door Raad van Bestuur

## 1 Wachtwoordbeleid – Phishing: hengelen naar gegevens ...

### 1.1 Wat is phishing?

Je zal zelf weleens een e-mail hebben gekregen die leek te komen van de bank of het telecombedrijf waar je al dan niet klant bij bent. In de mail wordt meestal gevraagd om op een link te klikken en dan je persoonlijke gegevens zoals naam, pincode, bankgegevens, wachtwoord... in te vullen. Waarschijnlijk word je in de mail ook gevraagd om het snel te doen. De reden die de mail opgeeft zijn uiteenlopend maar klinken heel realistisch: bijvoorbeeld omdat je achterstaande betalingen hebt en je anders een boete krijgt, of omdat er verdachte activiteiten zijn opgemerkt omtrent het gebruik van je kredietkaart maar het kan ook gewoonweg gaan omdat we je gegevens willen controleren.

Het aanmanen om het snel te doen is wel heel cruciaal omdat jij dan gewoon minder snel nadenkt en sneller gaat 'bijten'.

Eens je echter op de link klikt, word je naar een valse website geleid die lijkt op het officiële portaal: een gespoofde website. Meestal een nagemaakte website met een adres dat enorm goed lijkt op de originele (voorbeeld zou zijn [www.beltius.be](http://www.beltius.be) i.p.v. [www.belfius.be](http://www.belfius.be)) Indien je daar je gegevens zou invullen, worden ze rechtstreeks naar een cybercrimineel gestuurd die uit is op jouw informatie. Het kan ook dat je via de link malware op je computer krijgt, zoals een keylogger die je informatie bijhoudt, of ransomware, die je bestanden of je volledige computer versleutelt.

Dat is een voorbeeld van phishing, maar het fenomeen beperkt zich allerminst tot die exacte situatie. Phishing is een vorm van social engineering waarbij een cybercrimineel gegevens of geld van een gebruiker probeert te stelen. En dat kan op heel veel verschillende manieren.

### 1.2 Soorten phishing

Phishing gebeurt meestal via e-mail, hoewel het ook via een app, valse website, of ook telefonisch kan. Hieronder de meest voorkomende soorten:

**Spearphishing:** Leunt erg aan bij standaardphishing, alleen gaat het hier niet om een willekeurig doelwit. Een specifiek slachtoffer wordt uitgekozen en het bericht wordt gepersonaliseerd om de persoon te doen geloven dat het om een legitieme boodschap gaat. Vaak doet men wat social engineering om jou te doen geloven dat de mail afkomstig is van je baas of van een bepaalde persoon uit je werkomgeving die je vertrouwt.

**Whaling:** Spearphishing, maar dan gericht op de "grote vissen": managers, directeurs, CEO's, CFO's, en dergelijke. In plaats van één werknemer in de luren te leggen, mikt deze aanval op het groffe geld. De login-gegevens van de managers kunnen immers gebruikt worden om bedrijfskritische gegevens te stelen of phishing-mails naar honderden werknemers tegelijkertijd te sturen. Wie gaat er ooit een mail weigeren die effectief van de CEO komt?

**Pharming:** In plaats van te vissen, kiezen sommige cybercriminelen er ook voor om te oogsten. Met pharming worden nietsvermoedende gebruikers bij het surfen omgeleid. Dat kan bijvoorbeeld door een gehackte DNS-server. Zelfs wanneer de gebruiker dan de juiste url ingeeft, wordt hij nog omgeleid naar een valse website. Doelwitten zijn bijvoorbeeld de website van je bank, of van een sociaal netwerk. Wanneer je inlogt, zijn je gegevens niet langer privé.

### 1.3 Hoe herken je phishing?

Enkele jaren terug was het nog niet eens bijster moeilijk om een phishing-mail te herkennen, vooral niet in het Nederlands. De taal die werd gebruikt in de mail was vaak doorspekt met spelfouten en grammaticale flaters op een manier die zelfs de grootste taalbarbaar nauwelijks kon ontgaan. De huidige trend geeft echter aan dat cybercriminelen iets meer werk steken in de geloofwaardigheid van hun phishingmails. Veel van die mails zijn haast niet te onderscheiden van de real deal. Je kan wel een paar stappen overlopen om twijfel uit te sluiten.

**Let op de begroeting:** Rudimentaire phishing-mails die in bulk worden verzonden, beginnen vaak met een heel generische begroeting, zoals “Geachte klant” of “Beste collega”. Het is geen waterdicht signaal, aangezien spearphishing-mails wel gepersonaliseerd zijn, maar er moet een lampje gaan branden als het zo is.

**Wat wordt er gevraagd:** Een echte bank, telecombedrijf of andere instantie zal nooit via e-mail vragen om je gegevens te bevestigen, of andere informatie in te geven, via een link. Als het bovendien dringend moet, kan je ervanuit gaan dat ze zullen bellen.

**Check de link:** De link in phishing-mails beschrijft vaak de officiële pagina in de linktekst, maar leidt eigenlijk naar een heel andere website. Controleer de eindbestemming door over de link te zweven. Je kan de url dan linksonder in de hoek van je scherm bekijken.

Bij twijfel kan je altijd bellen naar de officiële instantie zelf. Doe dat dan aan de hand van een telefoonnummer dat je op een onafhankelijke website vindt, en dus niet het nummer dat eventueel in de mail te vinden is. Als je belt, kan de organisatie makkelijk zeggen of de mail legitiem is, of niet, en kunnen ze toekomstige klanten sneller waarschuwen voor frauduleuze e-mails.

## 2 *Communicatiebeleid – Netiquette*

Bron: [https://www.leren.nl/rubriek/computers\\_en\\_internet/internetten/nettiquette/](https://www.leren.nl/rubriek/computers_en_internet/internetten/nettiquette/)

### 2.1 Wanneer wel e-mail, wanneer niet?

‘Uit onze administratie blijkt dat uw dienstverband bij de Rijksuniversiteit is beëindigd’. Dit bericht vonden de 7.000 medewerkers van de Rijksuniversiteit Groningen op een maandagochtend in november 2006 in hun mailbox. Gelukkig bleek het om 'fout' in het computersysteem' te gaan. Waarom het automatisch gegenereerde mailtje naar duizenden medewerkers was gestuurd, was een groot raadsel. Nadat de fout was ontdekt, volgde meteen een excuusmail waarin de medewerkers werd verzekerd dat het een foutief bericht betrof en zij zich geen zorgen hoefden te maken over hun baan. De hele affaire had honderden bezorgde telefoontjes en e-mails tot gevolg.

Minder fortuinlijk waren de 400 medewerkers van een Amerikaanse elektronica keten RadioShack in september 2006. Zij werden per e-mail op de hoogte gebracht van hun ontslag en konden meteen hun spullen pakken. ‘Omwille van de efficiency’, had de directie van het bedrijf voor deze werkwijze gekozen. De medewerkers waren woedend en vonden de werkwijze ‘onmenselijk en respectloos’.

E-mail is in lang niet elke situatie het juiste communicatiemiddel. Denk bijvoorbeeld aan zaken die iemand persoonlijk raken, zoals de beëindiging van een dienstverband. Dit hoort in een persoonlijk gesprek besproken te worden. Of als je een vraag hebt waar je meteen antwoord op wilt, kun je beter de telefoon pakken of even bij je collega langsgaan en het hem vragen. Toch wordt e-mail regelmatig gebruikt in situaties waarin een persoonlijk gesprek beter op zijn plaats was geweest. Niet zelden leidt dit - vaak ondoordacht – automatisme tot irritaties, woede en misverstanden. Vraag je bij elk bericht even af of het wel verstandig is voor de betreffende boodschap e-mail als medium te gebruiken.

#### **Situaties waarin je e-mail kunt gebruiken**

Je kunt je mail gebruiken als je:

- Een afspraak wilt maken met 1 of meerdere personen
- Een afspraak wilt bevestigen
- Een eenvoudige vraag hebt
- Een vraag hebt waar je niet snel een antwoord op hoeft te krijgen
- Een antwoord moet geven op een eenvoudige vraag
- Aan veel mensen tegelijk een mededeling wilt doen (en die niet heel belangrijk is)
- Een vergadering wilt plannen
- Iemand wilt bereiken die heel slecht bereikbaar is.

#### **Situaties waarin je e-mail beter niet kunt gebruiken**

Je kunt je mail beter niet gebruiken als je:

- Een meningsverschil hebt
- Vertrouwelijke informatie wilt uitwisselen
- Slecht nieuws hebt
- In een situatie zit waar een probleem bestaat of dreigt te ontstaan
- Op het allerlaatste moment een vergadering of afspraak wilt afzeggen
- Veel vragen hebt

- Een vraag hebt waar je met spoed een antwoord op wilt hebben
- Een vervelend bericht hebt.

### **Andere mogelijkheden**

Wat kun je doen als e-mail niet het meest geschikte medium is?

- Loop bij je collega langs
- Pak de telefoon
- Maak een afspraak voor een persoonlijk gesprek
- Verstuur de informatie via de (interne) post
- Spreek je collega aan

## 2.2 Do's van e-mailen

Je typt een bericht, kiest een adres, drukt op verzenden en... klaar. Een kind kan de was doen. E-mail heeft haar populariteit te danken aan het gemak en de snelheid waarmee een berichtje kan worden verstuurd. Maar juist daardoor gaat het ook zo vaak mis: in de haast opgestelde berichten vol spelfouten, onduidelijke verzoeken en nutteloze mededelingen leiden tot irritatie, volle inboxen en veel tijdverlies, want al die e-mails moeten toch geopend en bekeken worden.

### **Wees helder en to the point**

Verplaats je in de ontvanger van je e-mail en geef in de onderwerpregel bovenaan het bericht aan waar het over gaat. Je kunt bijvoorbeeld aangeven wat je van hem verlangt en - zonodig - wanneer. Ook kun je (duidelijk!) verwijzen naar eerdere e-mails. Bijvoorbeeld: '... in mijn mail van 24 september jl. met als onderwerp 'concept beleidsnota versie 1.2''. Het is dan voor de ontvanger meteen duidelijk of hij snel actie moet ondernemen of dat je bericht even kan wachten. Bovendien kan hij je bericht zo gemakkelijk terugvinden. Hiermee toon je niet alleen respect voor de tijd van een ander, je ontvangt waarschijnlijk ook een helder antwoord terug. Probeer je zoveel mogelijk tot één onderwerp te beperken. Heb je meerdere onderwerpen, spreid ze dan over meerdere e-mails. De ontvanger houdt zo het overzicht en kan je e-mails gemakkelijker afhandelen. Behandel je toch meer onderwerpen in je bericht, geef de onderwerpen dan een nummer.

Kom in de eerste alinea van je e-mailbericht meteen to-the-point. Wil je dat je collega de tweede versie van je concepttekst van commentaar voorziet, geef dat dan aan. Eventuele toelichting kun je daarna geven. Houd je bericht zo kort mogelijk, want het lezen van lange lappen tekst op een beeldscherm is niet prettig. Dreigt je e-mail toch erg lang te worden, voorzie je tekst dan van tussenkopjes.

Heb je dringend een reactie nodig, bel dan de ontvanger ook even om te zeggen dat je een e-mail hebt gestuurd. Je kunt zo de urgentie van je bericht nog eens benadrukken en de ontvanger kan aangeven of hij binnen de door jouw gestelde termijn kan reageren.

Overigens: gebruik voor de echte spoedgevallen niet de e-mail, maar pak de telefoon of loop even bij je collega langs.

### **Ga weloverwogen met bijlagen om**

Met de bijlagenfunctie in je e-mailprogramma kun je bestanden met je e-mail meesturen. Hartstikke handig, alleen moet je ze wél daadwerkelijk toevoegen; het is weinig professioneel wanneer je in je e-mail naar een attachment verwijst dat ontbreekt. Je kunt dit voorkomen door er een gewoonte van te maken eerste de bijlage te selecteren en daarna pas het begeleidende bericht te schrijven. Schrijf altijd een begeleidende tekst bij een bijlage. Hierin leg je het doel van de bijlage uit en geef je precies aan wat je van de ontvanger verwacht.

Vraag je altijd af of het nodig is om de bijlage met je bericht mee te sturen. Staat de informatie al op het intranet of in een gedeelde map, dan is een link hiernaar voldoende. Zo voorkom je onnodig geheugengebruik in de mailbox van de ontvanger en overbelasting van het bedrijfsnetwerk. Bovendien hoeft de ontvanger minder handelingen te verrichten (bijlage openen, opslaan, verwijderen).

Wanneer je een bijlage meestuurt, let er dan op dat het bestand een duidelijke naam heeft en niet te groot is. Nietszeggende bestanden, zoals verslag.doc, en grote bestanden die niet snel geopend kunnen worden, wekken irritaties op bij de ontvanger. Nog erger is het wanneer je bijlage een virus blijkt te bevatten. Controleer bijlagen dan ook altijd op grootte en virussen.

### **Beperk het gebruik van cc**

In sommige organisaties slibben inboxen helemaal dicht door de enorme hoeveelheid cc'tjes die worden verstuurd. Veelal heeft dit met de bedrijfscultuur te maken. Wees selectief in het versturen van zogenoemde cc'tjes. Gebruik cc alleen als het echt nodig is voor de ontvanger.

### **Let op correcte adressering**

In de haast kan het wel eens gebeuren dat je een adres verkeerd intikt, de verkeerde contactpersoon in je adresboek selecteert of iemand vergeet. Controleer bij het verzenden van een bericht altijd of je het bericht aan de juiste perso(o)n(en) hebt geadresseerd. Vooral bij gevoelige informatie kan een dubbele check geen kwaad. Voorzie externe mail altijd van een disclaimer. In het geval een bericht bij de verkeerde persoon wordt bezorgd, zorgt deze ervoor dat derden hieraan geen rechten kunnen ontlenen of het bedrijf aansprakelijk kunnen stellen.

### **Let op formulering en spelling**

Gaan we voor een brief nog eens goed zitten, bij het schrijven van een e-mail lijken goede omgangsvormen en spellingsregels te verdwijnen als sneeuw voor de zon: berichten vol spelfouten waarin alleen het hoognodige wordt vermeld. Hoewel zo niet bedoeld, kun je bij de ontvanger zo ongenueanceerd en kortaf overkomen.

Natuurlijk maakt het uit naar wie je de e-mail verstuurt - een snelle boodschap aan een collega kan informeler dan een bericht aan een klant - maar een correcte spelling en een goede formulering is ook een kwestie van fatsoen. Bovendien kom je met een goed geformuleerd en een juist gespelde tekst professioneler over dan met een rommelig bericht. Lees een e-mail dus goed door voor je hem verzendt en gebruik je spelling- en grammaticacontrole.

Wees ook voorzichtig met ironie, sarcasme en humor. Door het ontbreken van fysiek contact kan een grap gemakkelijk als kritiek overkomen.



## 2.3 Don'ts van emailen

### **Zet de ontvanger niet op het verkeerde been**

Verstuur nooit een e-mail zonder het onderwerp in de onderwerpregel aan te geven. Verzend ook nooit een bericht zonder je naam te vermelden. Schrijf geen zinnen in hoofdletters. De ontvanger zal dit interpreteren als schreeuwen en zal denken dat je boos op hem bent.

### **Gebruik e-mail niet voor gevoelige onderwerpen of slecht nieuws**

Hoewel e-mail in lastige situaties een aantrekkelijk alternatief lijkt, mag je je nooit achter een e-mail verschuilen. Door het ééndimensionale karakter van e-mail zie je niet hoe je bericht bij de ontvanger overkomt en kun je een misverstand niet meteen rechtzetten. Ook heb je geen idee van de omstandigheden en timing van het moment waarop je e-mail wordt gelezen.

### **Verzend geen vertrouwelijke informatie**

In principe is e-mail niet geschikt voor het uitwisselen van vertrouwelijke informatie. Ook privé-informatie over collega's wissel je niet uit via de mail. Een e-mail - of de reactie daarop – wordt nogal eens naar anderen doorgestuurd en dan komt je bericht terecht bij mensen voor wie jij hem niet had bestemd. Wees je ervan bewust dat in veel organisaties de systeembeheerder toegang heeft tot je e-mail.

### **Bcc**

Wanneer je een bericht aan meerdere zakelijke contacten verstuurt, is het niet zo professioneel als de e-mailadressen van de geadresseerden voor iedereen zichtbaar zijn. Er zijn organisaties die maar al te gemakkelijk gebruikmaken van deze adressen om spam te versturen. Gebruik in een dergelijk geval bcc (blind carbon copy). De adressen die je hier invoert, zijn dan niet zichtbaar voor de anderen.

### **Wees niet te gemakzuchtig**

Stuur niet voor ieder wissewasje een e-mail. Vraag je bij elk bericht even af of het wel verstandig is voor de betreffende boodschap e-mail als medium te gebruiken. Is een telefoontje of rechtstreeks contact met de collega, die een paar kamers verderop zit niet effectiever? En hoewel het een verleidelijk alternatief is om niet zelf de archiefkast in te hoeven duiken, is het niet verstandig om een e-mail te versturen waarin je om informatie vraagt die je zelf gemakkelijk kunt opzoeken. Het is niet collegiaal en zal voor de nodige irritaties kunnen zorgen.

### **Cc**

Vele inboxen slibben dicht door de grote hoeveelheid cc'tjes die 'voor de zekerheid' en 'ter info' worden verstuurd. Doe hier niet aan mee en wees selectief in het versturen van cc'tjes.

### **To: alle afdelingen**

In veel organisaties is het mogelijk om een bericht te versturen naar alle medewerkers of de medewerkers van een organisatieonderdeel, bijvoorbeeld de afdeling IT of Personeelszaken. Dat kan erg efficiënt zijn, bijvoorbeeld wanneer de directie een belangrijk bericht heeft.

Maar al te vaak wordt deze mogelijkheid uit gemakzucht gebruikt, omdat de verzender van de e-mail niet goed weet aan wie hij zijn bericht moet richten en voor het gemak de hele afdeling maar adresseert. Een bron van onnodige frustratie bij alle niet-terechte ontvangers.

## Gebruik e-mail niet voor niet-zakelijke mail

Kettingbrieven horen niet thuis op het werk. Dat geldt ook voor e-mails die kwetsend kunnen zijn door grappen over huidskleur, afkomst, religie, seksuele geaardheid, ras of sekse. Gebruik je e-mail op het werk ook niet voor het verhandelen van spullen.

### 2.4 Checklist do's en don'ts

Do's	Don'ts
<p>Let op formulering en spelling</p> <ul style="list-style-type: none"> <li>• Wees voorzichtig met ironie, sarcasme en humor</li> <li>• Voorkom spellingsfouten: lees je e-mail voor verzenden goed door en gebruik de spellingcontrole</li> </ul> <p>Wees helder en to the point</p> <ul style="list-style-type: none"> <li>• Zet in de onderwerpregel wat je van de ontvanger verwacht en wanneer</li> <li>• Begin je e-mail met je boodschap gevolgd door een toelichting</li> <li>• Behandel één onderwerp per e-mail</li> <li>• Behandel je meer onderwerpen per e-mail, nummer de onderwerpen dan</li> <li>• Houd je e-mail kort en zakelijk</li> <li>• Vraagt je e-mail echt snelle actie, bel dan de geadresseerde ook even op</li> </ul> <p>Ga weloverwogen met bijlagen om</p> <ul style="list-style-type: none"> <li>• Schrijf altijd een begeleidende tekst bij een bijlage: leg hierin uit wat het doel van de bijlage is en wat je van de ontvanger verwacht.</li> <li>• Vergeet de bijlage niet mee te sturen: leer jezelf aan eerst de bijlage te selecteren, daarna stel je de begeleidende mail op</li> <li>• Vraag je af of het noodzakelijk is om de bijlage toe te voegen of alleen een link voldoende is</li> <li>• Voorzie de bijlage van een duidelijke naam</li> <li>• Controleer bijlagen altijd op grootte en virussen</li> </ul> <p>Beperk het gebruik van cc</p> <ul style="list-style-type: none"> <li>• Gebruik cc alleen als het echt nodig is voor de ontvanger.</li> </ul> <p>Let op correcte adressering</p> <ul style="list-style-type: none"> <li>• Controleer altijd of je je e-mail aan de juiste perso(n)en adresseert</li> </ul>	<p>Zet de ontvanger niet op het verkeerde been</p> <ul style="list-style-type: none"> <li>• Verstuur nooit een e-mail zonder het onderwerp in de onderwerpregel aan te geven</li> <li>• Verzend ook nooit een e-mail zonder je naam te vermelden</li> <li>• Schrijf geen zinnen in hoofdletters</li> <li>• Verschuil je nooit achter een e-mail</li> </ul> <p>Verzend geen vertrouwelijke informatie</p> <ul style="list-style-type: none"> <li>• Verzend geen vertrouwelijke informatie of privé-informatie over collega's</li> <li>• Stuur e-mailadressen niet open en bloot mee als je een bericht verstuurt naar meerdere externe contacten</li> </ul> <p>Wees niet te gemakzuchtig</p> <ul style="list-style-type: none"> <li>• Stuur niet voor ieder wisselwasje een e-mail</li> <li>• Vraag niet om informatie die je zelf gemakkelijk had kunnen opzoeken</li> <li>• Verstuur niet aan een hele afdeling een e-mail als je niet precies weet aan wie je je bericht moet richten</li> <li>• Wees niet gemakkelijk in het versturen van cc'tjes</li> </ul> <p>Gebruik e-mail niet voor niet-zakelijke mail</p> <ul style="list-style-type: none"> <li>• Doe niet mee aan kettingbrieven of andere 'grappen'</li> <li>• Gebruik je e-mail niet voor het verhandelen van spullen</li> </ul>