

Informatiebeveiliging en privacy beleid

De Stroming



Versie: 28 juni 2018, na Directie Beraad d.d. 26 juni 2018
Bron: Kennisnet

	Directieberaad	College van Bestuur	Raad van Toezicht	Gemeenschappelijke Medezeggenschapsraad
Vergaderdatum	26 juni 2018	3 juli 2018	28 januari 2019	22 januari 2019
Besluitvorming	<i>Advies</i>	<i>Vaststellen</i>	<i>Goedkeuren</i>	<i>Instemming</i>

INHOUDSOPGAVE

1	INLEIDING.....	3
1.1	Informatiebeveiliging en privacy	3
1.2	Doel	3
2	UITGANGSPUNTEN	4
2.1	Privacy	4
3	WET- EN REGELGEVING	5
4	ORGANISATIE	6
4.1	Richtinggevend	6
4.2	Sturend	6
4.3	Uitvoerend	6
5	CONTROLE EN RAPPORTAGE	8
5.1	Voorlichting en bewustzijn	8
5.2	Classificatie en risicoanalyse.....	8
5.3	Incidenten en datalekken.....	8
5.4	Controle, naleving en sancties	8

Bijlage A: Tabel IBP rollen en taken

1 INLEIDING

Informatie en ICT zijn noodzakelijk in de ondersteuning van ons onderwijs. Omdat we met persoonsgegevens (van onszelf, leerlingen en anderen) werken, is privacywetgeving daarop van toepassing.

De informatie en ICT van De Stroming worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan worden bedreigd door een aanval, een vergissing, de natuur (bijv. overstroming of brand), et cetera. Het niet beschikbaar zijn van ICT, incorrecte administraties en het uitlekken van gegevens kan tot inbreuken leiden op het geven van onderwijs en het vertrouwen in onze scholen.

Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Om dit structureel op te pakken is het noodzakelijk dat we duidelijk maken waar het om gaat, doelen stellen met betrekking tot de reductie van de risico's en de manier vaststellen waarop we deze doelen willen bereiken.

1.1 Informatiebeveiliging en privacy

Informatiebeveiliging is een proces voor het beschermen van De Stroming tegen risico's en bedreigingen met betrekking tot informatie en ICT. Het richt zich op drie aspecten:

- Beschikbaarheid; informatie en aanverwante bedrijfsmiddelen zijn toegankelijk wanneer nodig;
- Integriteit; informatie en verwerkingsmethoden bevatten zo min mogelijk fouten;
- Vertrouwelijkheid; informatie is alleen toegankelijk voor diegene die daartoe bevoegd zijn.

Privacy gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving. Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan. Vooral het aspect vertrouwelijkheid is hiervoor van belang. Informatiebeveiliging is daarom integraal onderdeel van privacy.

Om privacy goed te regelen is informatiebeveiliging nodig. Daarom zien we het als één onderwerp: informatiebeveiliging en privacy (IBP).

1.2 Doelen

Dit beleid heeft als doelen:

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

Dit beleid is een leidraad voor iedereen die betrokken is bij IBP binnen De Stroming. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen binnen De Stroming. Het is van toepassing op de hele organisatie van De Stroming, waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.

Het informatiebeveiligings- en privacybeleid heeft raakvlak met andere beleidsgebieden, te weten:

- Algemeen veiligheids- en beveiligingsbeleid; met als aandachtsgebieden bedrijfshulpverlening, fysieke toegang en -beveiliging, crisismanagement, huisvesting en ongevallen;
- Informatietechnologie-beleid; met als aandachtsgebieden de aanschaf en het beheer van ICT;
- Personeels- en organisatiebeleid; met als aandachtsgebieden in- en uitstroom van medewerkers, functiescheiding en vertrouwensfuncties;

Dit beleid maakt duidelijk waar de verantwoordelijkheden rondom informatiebeveiliging en privacy zijn belegd.

2 UITGANGSPUNTEN

De belangrijkste beleidsuitgangspunten bij De Stroming zijn:

- Informatiebeveiliging en privacy dienen te voldoen aan alle relevante wet- en regelgeving;
- Veilig en betrouwbaar omgaan met informatie is de verantwoordelijkheid van iedereen;
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid;
- De Stroming is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt;
- De Stroming maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy;
- IBP is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is;
- Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen;
- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid.

2.1 Privacy

De Stroming hanteert de vijf vuistregels voor privacy:

1. **Doelbepaling en doelbinding:** persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag:** verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie:** bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie:** de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.

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

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

3 WET- EN REGELGEVING

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

- Wet op het primair onderwijs
- Wet goed onderwijs en goed bestuur PO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 2.0' leidend bij het maken van afspraken met leveranciers.

4 ORGANISATIE

Dit hoofdstuk beschrijft hoe IBP binnen De Stroming is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

4.1 Richtinggevend

Het College van Bestuur (CvB; de Bestuurder) is eindverantwoordelijk voor IBP en stelt het beleid en de maatregelen vast op het gebied van informatiebeveiliging en privacy. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages door de bestuurder geëvalueerd.

4.2 Sturend

4.2.1 Directiebestuur (DB)

Het directiebestuur heeft een rol op sturend niveau. Het directiebestuur bestaat uit de directeuren van de scholen en de beleidsmedewerker HRM en wordt voorgezeten door de Bestuurder (CvB). Het directiebestuur geeft terugkoppeling en advies aan de bestuurder en stuurt de mensen aan op de uitvoerende laag. Verantwoordelijkheden van het directiebestuur:

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

4.2.2 Functionaris voor Gegevensbescherming

De externe functionaris voor gegevensbescherming (FG) houdt binnen De Stroming toezicht op de toepassing en naleving van de privacy-wetgeving. De externe FG heeft daarmee een onafhankelijke positie in de organisatie. De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. FG heeft regelmatig overleg met het directiebestuur. De FG is meestal ook contactpersoon voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.

4.2.3 Domeinverantwoordelijkheid/proceseigenaar

Binnen de scholen zijn er verschillende domeinen/processen, zoals ICT, personeel, administratie et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Leidinggevenden hebben een voorbeeldrol ten opzichte van hun medewerkers.

4.3 Uitvoerend

4.3.1 Beleidsmedewerker online veiligheid

De beleidsmedewerker online veiligheid vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging.

4.3.2 Functioneel beheerder

Op basis van de domeinverantwoordelijke/proceseigenaar heeft de functioneel beheerder een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

4.3.3 Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in het personeelshandboek en de handleiding aanvaardbaar gebruik van bedrijfsmiddelen. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers worden onder andere gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via het medezeggenschapsorgaan)

4.3.4 Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere directeur* heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn of haar medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij of zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De directeur kan in zijn taak ondersteund worden door (leden van) het directieberaad.

* Op scholen met teamleiders kunnen taken worden gedelegeerd aan hen.

5 CONTROLE EN RAPPORTAGE

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door het directiebestuur. Hierbij wordt rekening gehouden met:

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

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

5.1 Voorlichting en bewustzijn

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

5.2 Classificatie en risicoanalyse

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

5.3 Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij avg@destroming.eu. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken.

5.4 Controle, naleving en sancties

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

Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de bestuurder, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het CvB vast te stellen reglement.

Mocht de naleving ernstig tekort schieten, dan kan De Stroming de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de cao en de wettelijke mogelijkheden.

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

Bijlage A Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	College van Bestuur	<ul style="list-style-type: none"> • Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten 	<ul style="list-style-type: none"> • Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	Directiebestuur	<ul style="list-style-type: none"> • Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert CvB over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen 	Processen, richtlijnen en procedures IBP, waaronder: <ul style="list-style-type: none"> • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Bewerksvereenkomsten regelen • Brief toestemming gebruik foto's en video • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ICT en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming	<ul style="list-style-type: none"> • Toezicht op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten 	<ul style="list-style-type: none"> • Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
	Domein-verantwoordelijke / Proceseigenaren waaronder: ICT, personeel (HRM), onderwijs, financiën, inkoop, administratie	<ul style="list-style-type: none"> • Classificatie / risicoanalyse <i>in samenwerking FG en CvB.</i> • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door CvB. • <i>Samen met functioneel beheer en ICT beheer</i> er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • <i>Samen met functioneel beheer en ICT beheer</i> de toegangsrechten van gebruikers regelmatig beoordelen en controleren. 	<ul style="list-style-type: none"> • Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: <ul style="list-style-type: none"> • Toegangsmatrix diverse informatiesystemen en netwerk

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Uitvoerend (operationeel)	Functionaris Gegevensbescherming ICT beheerder Functioneel beheerder Medewerker Directeuren	<ul style="list-style-type: none"> • Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur. 	Communiceren, informeren en toezien op naleving van o.a.: <ul style="list-style-type: none"> • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken