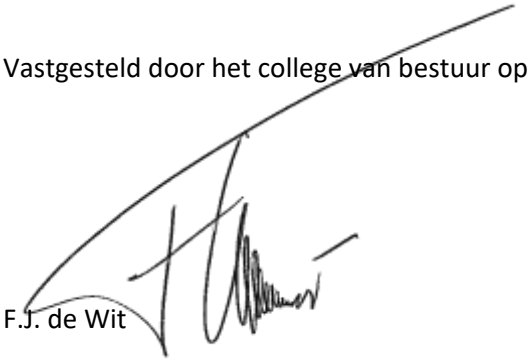
# Informatiebeveiligings- en privacy beleid

## Stichting Scala College en Coenecoop College

Vastgesteld door het college van bestuur op 6 juni 2019



F.J. de Wit

Instemming GMR 05-06-2019
Revisie 02-02-2022

| Versie | Status | Datum | Auteur | Omschrijving |
|---|---|---|---|---|
| 0.1 | Concept | 26/03/2019 | Bron: Kennisnet, bewerkt voor Stichting Scala College en Coenecoop College door Roland Sturkenboom | 1e concept voor review Werkgroep IBP |
| 0.2 | Concept | 09/04/2019 | Roland Sturkenboom | 2e concept; review Bestuurder |
| 0.3 | Concept | 16/04/2019 | Roland Sturkenboom | 3e concept; ter bespreking in MT 16/05/2019 |
| 0.4 | Concept | 21/05/2019 | Roland Sturkenboom | 4e concept; ten behoeve van GMR, ter bespreking en verzoek om instemming |
| 1.0 | Definitief | 06/06/2019 | | Vastgesteld door het college van bestuur, met instemming van de GMR |

# 1 Het belang van informatiebeveiliging en privacy en de privacy-missie

## 1.1 Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

## 1.2 De privacy-missie van Stichting Scala College en Coenecoop College

Stichting Scala College en Coenecoop College (hierna genoemd: Stichting Scala en Coenecoop) heeft als vertrekpunt voor zijn privacy-beleid de volgende privacy-missie geformuleerd:
*Stichting Scala en Coenecoop behandelt haar leerlingen, medewerkers en relaties met respect. Stichting Scala en Coenecoop gaat daarom integer, transparant, professioneel en zorgvuldig om met persoonsgegevens. Zij verwerkt deze in overeenstemming met haar kwaliteitsbeleid en met wet- en regelgeving op het gebied van de bescherming van Persoonsgegevens, zoals de Algemene Verordening Gegevensbescherming (AVG).*

# 2 Toelichting informatiebeveiliging en privacy

## 2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:

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

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

Uit oogpunt van de kwaliteit van de informatievoorziening, hecht Stichting Scala en Coenecoop er daarnaast waarde aan dat de informatie in haar systemen en bestanden steeds zo *actueel* mogelijk is.

### 2.2 Toelichting privacy

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

### 2.3 Samenhang informatiebeveiliging en privacy

Informatiebeveiliging en de bescherming van persoonsgegevens zijn nauw met elkaar verbonden en worden daarom samengevoegd in één organisatieproces, informatiebeveiliging en privacy; hierna verder afgekort tot IBP. Het is dan ook logisch hiervoor een samenhangend beleid te formuleren en te hanteren: het informatiebeveiligings- en privacy-beleid (het IBP-beleid).
Dit vormt als het ware de kapstok voor de verdere uitwerking in richtlijnen, procedures en protocollen.

## 3 Doelen, reikwijdte en uitgangspunten van het IBP-beleid

### 3.1 Doelen

Het IBP-beleid van Stichting Scala en Coenecoop heeft de volgende doelen:

- Het waarborgen van de continuïteit en kwaliteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Stichting Scala en Coenecoop persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

### 3.2 Reikwijdte

- Het IBP-beleid geldt voor alle medewerkers, leerlingen, ouders/verzorgers, stagiairs, vrijwilligers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting Scala en Coenecoop waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting Scala en Coenecoop persoonsgegevens verwerkt.

- Het IBP-beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting Scala en Coenecoop. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en in beginsel ook niet-gecontroleerde informatie waarop de school kan worden aangesproken.

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Stichting Scala en Coenecoop evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- Het IBP-beleid heeft binnen Stichting Scala en Coenecoop onder meer raakvlakken met:
  - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
  - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
  - *ICT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
  - *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

### 3.3 Uitgangspunten

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

1. Stichting Scala en Coenecoop streeft naar een juiste balans tussen privacy, functionaliteit en veiligheid. In overeenstemming met de hiervoor geformuleerde privacy-missie blijft een belangrijk vertrekpunt daarbij altijd, dat de persoonlijke levenssfeer van de betrokkenen (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en dat Stichting Scala en Coenecoop voldoet aan alle relevante wet- en regelgeving.

2. Als verwerkingsverantwoordelijke in de zin van de wet, neemt het bevoegd gezag van Stichting Scala en Coenecoop (oftewel: het College van Bestuur) de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld worden. Het College van Bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de privacywetgeving is het College van Bestuur de verwerkingsverantwoordelijke. Tegelijkertijd is binnen Stichting Scala en Coenecoop het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.

3. Stichting Scala en Coenecoop voldoet aan alle, voor het IBP-beleid, relevante wet- en regelgeving, waaronder:
   - Algemene Verordening Gegevensbescherming (AVG)
   - Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)
   - Wet voortgezet onderwijs
   - Wet goed onderwijs en goed bestuur PO/VO
   - Wet onderwijstoezicht
   - Wet medezeggenschap op scholen
   - Jeugdwet
   - Leerplichtwet
   - Archiefwet

- Auteurswet
- Wetboek van Strafrecht

4. Stichting Scala en Coenecoop is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

5. Ook als het gaat om het respecteren van de privacy van anderen, verwacht Stichting Scala en Coenecoop van alle medewerkers, leerlingen, ouders, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' en verantwoordelijk gedrag. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies voor mede-betrokkenen en/of de onderwijsinstelling. Richtlijnen voor leerlingen zijn onder andere opgenomen in het leerlingenstatuut en in protocollen voor omgangsvormen en gebruik van ICT-middelen. Richtlijnen voor medewerkers zijn onder andere opgenomen in gedragscodes. En specifiek voor het verwerken van persoonsgegevens gelden voor medewerkers de basisprincipes en gedragsregels zoals hierna onder 4.1 geformuleerd.

6. Informatiebeveiliging en privacy is bij Stichting Scala en Coenecoop een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

# 4 Uitwerking van het beleid – het hoe en wat

Dit hoofdstuk geeft een praktische invulling van bovenstaande uitgangspunten en is daarmee de uitwerking van het IBP-beleid op hoofdlijnen.

## 4.1 Basisprincipes en gedragsregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de principes leidend, die door de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) zijn vastgelegd; de zgn. *Fair Information Principles*. Deze principes zijn ook het fundament van de nieuwe privacywetgeving, de AVG. Op basis hiervan gelden er voor Stichting Scala en Coenecoop samengevat de volgende **tien gedragsregels** met betrekking tot de omgang met persoonsgegevens:

1. Wij beperken ons bij het verzamelen van persoonsgegevens tot enkel die gegevens die wij op rechtmatige wijze en met redelijke middelen heeft verkregen en indien van toepassing altijd met kennis of toestemming van de betrokkenen.

2. Wij zorgen er voor dat de door ons verzamelde persoonsgegevens beperkt blijven tot de doelen waarvoor ze worden verzameld en dat deze steeds juist, compleet en up-to-date zijn.

3. Wij verzamelen enkel persoonsgegevens nadat:
    a. de doelen van het verzamelen afdoende en op voorhand bekend zijn gemaakt;
    b. duidelijk is dat het gebruik beperkt wordt tot het realiseren van deze doelen; OF
    c. tot andere (van geval tot geval gespecificeerde) doelen die niet strijdig zijn met het doel waarvoor ze eerder werden verzameld.

4. Wij stellen geen persoonsgegevens ter beschikking voor andere doelen dan waarvoor ze zijn verzameld, behalve dan op grond van:
    a. expliciet door de betrokkene gegeven toestemming;
    b. een wettelijke verplichting.

5. Wij zorgen er voor dat de aan ons ter beschikking gestelde persoonsgegevens passend worden beveiligd tegen verlies, vernietiging, ongeautoriseerde toegang, ongeoorloofd gebruik, -veranderingen, of terbeschikkingstelling.

6. Wij communiceren proactief omtrent onze vestigingslocaties en ons privacybeleid, met inbegrip van de aard en reden van de verwerking van persoonsgegevens en de rechten van betrokkenen.

7. Wij zorgen er voor dat iedere persoon die zich bij de school meldt:
    a. antwoord krijgt op de vraag of wij persoonsgegevens over hem/haar hebben;
    b. de feitelijke beschikking krijgt over deze hem/haar betreffende persoonsgegevens;
    c. deze gegevens in beginsel kosteloos en in een leesbare vorm krijgt;
    d. en indien hem/haar dit wordt geweigerd, dit onder vermelding van reden wordt geweigerd alsmede de wijze waarop hiertegen beroep kan worden aangetekend;
    e. de hem/haar betreffende persoonsgegevens kan aanvechten en -indien terecht- kan eisen dat deze persoonsgegevens worden verwijderd, gecorrigeerd, aangevuld of gewijzigd.

8. Wij zorgen er voor dat wij op ieder moment in staat zijn verantwoording af te leggen over de wijze waarop wij als organisatie invulling geven aan onze privacygedragsregels.

9. Wij zorgen er voor dat de door ons verzamelde persoonsgegevens niet langer worden bewaard dan nodig voor het realiseren van het/de op voorhand aangegeven doel(en) waarvoor ze zijn verzameld.

10. Wij dragen geen persoonsgegevens over naar een land of gebied buiten de EER landen, voordat wij ons er van hebben verzekerd dat het ontvangende land de rechten en vrijheden van betrokkenen, waar het de verwerking van persoonsgegevens betreft, afdoende waarborgt en beveiligt.

### 4.2 Ondersteunende richtlijnen, procedures en protocollen

Diverse richtlijnen, procedures en protocollen geven invulling aan het beleid. De meest actuele versies daarvan zijn gepubliceerd op de websites van Stichting Scala en Coenecoop en/of van de afzonderlijke scholen. Bijlage 1 geeft een overzicht van de diverse documenten die hetzij reeds zijn gepubliceerd, hetzij in ontwikkeling zijn, hetzij nog ontwikkeld zullen worden.

### 4.3 Verwerkingsregister

Stichting Scala en Coenecoop legt alle verwerkingen van persoonsgegevens vast in een verwerkingsregister en zal dit up-to-date houden. Stichting Scala en Coenecoop voldoet hiermee aan de documentatieplicht op grond van de AVG.

### 4.4 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers regelmatig aangescherpt, zodat de kennis van risico's bij het omgaan met persoonsgegevens wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en andere betrokkenen. Verhoging van het bewustzijn m.b.t informatiebeveiliging en privacy is een gezamenlijke verantwoordelijkheid van de schoolleiding, de afdeling ICT en de Functionaris Gegevensbescherming, met het College van Bestuur als eindverantwoordelijke.

### 4.5 Classificatie en risicoanalyse

Stichting Scala en Coenecoop classificeert informatie en informatiesystemen waarop het IBP-beleid van toepassing is. Deze classificatie is het uitgangspunt voor de risicoanalyse van de veiligheid van informatie en persoonsgegevens en voor de te nemen beveiligingsmaatregelen.

Bij de classificatie zijn beschikbaarheid, integriteit en vertrouwelijkheid de aspecten die van belang zijn. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie.
Voorafgaand aan de start van nieuwe (ICT)projecten, zoals wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, en voorafgaand aan nieuwe verwerkingen wordt gekeken naar de impact op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden om risico's te voorkomen of beperken. Hierbij moet er altijd een gezonde balans zijn tussen de risico's die Stichting Scala en Coenecoop wil afdekken en de benodigde investeringen verbonden aan de te nemen maatregelen.

### 4.6 Afspraken met verwerkers

Stichting Scala en Coenecoop sluit met alle leveranciers, waaronder die van digitale onderwijsmiddelen en bedrijfsapplicaties, verwerkersovereenkomsten af als zij, in opdracht van Stichting Scala en Coenecoop, persoonsgegevens verwerken. In termen van de AVG geldt Stichting Scala en Coenecoop dan als *verwerkingsverantwoordelijke* en de leveranciers als *verwerkers*.

Bij het afsluiten van deze verwerkersovereenkomsten zijn de bepalingen van de meest recente versie van het 'Convenant Digitale onderwijsmiddelen en privacy' voor Stichting Scala en Coenecoop zoveel mogelijk leidend.

### 4.7 Incidenten en datalekken

Stichting Scala en Coenecoop heeft een protocol voor de melding en afhandeling van beveiligingsincidenten en datalekken. Dit protocol omvat een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

### 4.8 Planning en controle

Dit IBP-beleid wordt in beginsel elke vier jaar getoetst en zonodig bijgesteld door het Bestuur. Hierbij wordt rekening gehouden met:

- de status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);

- de actuele geinventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

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

### 4.9 Naleving en sancties

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

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

### 4.10 Logging en monitoring

Logging en monitoring door de afdeling ICT zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk. Daarnaast legt de afdeling ICT de incidenten die gemeld zijn vast in het register voor informatiebeveiligingsincidenten en datalekken. Zie hiervoor ook onder 4.7.

# 5 Organisatie - Wie doet wat?

## 5.1 Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij speelt de verdeling van verantwoordelijkheden en taken en de samenwerkingsrelatie tussen de verschillende actoren (functies / rollen en afdelingen) binnen Stichting Scala en Coenecoop en de aangesloten scholen een belangrijke rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen binnen Stichting Scala en Coenecoop.

| Niveau | Wie<br>Rollen | Hoe<br>Verantwoordelijkheid / taken | Wat<br>Realiseren / vastleggen |
|---|---|---|---|
| **Richtinggevend (strategisch)** | college van bestuur (CvB) | • Eindverantwoordelijk<br>• IBP-beleidsvorming, -vastlegging en het uitdragen ervan<br>• Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens<br>• Evalueren toepassing en werking IBP-beleid op basis van rapportages<br>• Organisatie IBP inrichten | • Informatiebeveiligings- en privacy beleid<br>• Basismaatregelen<br>• Privacyreglement vaststellen |
| **Sturend (tactisch)** | Werkgroep IBP | • Inhoudelijk verantwoordelijk voor IBP<br>• IBP-planning en controle<br>• Adviseert college van bestuur over IBP<br>• Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse<br>• Hanteren IBP normen en wijze van toetsen<br>• Evalueren IBP-beleid en maatregelen<br>• Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze<br>• Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen | Processen, richtlijnen en procedures IBP, waaronder:<br>• Protocol beveiligingsincidenten en datalekken.<br>• Verwerkersovereenkomsten regelen<br>• Brief toestemming gebruik beeldmateriaal.<br>• Opstellen informatie documentatie richting leerlingen, ouders / verzorgers.<br>• Security awareness activiteiten.<br>• Sociale media reglement.<br>• Gedragscode ICT en internetgebruik.<br>• Gedragscode medewerkers en leerlingen. |
| | Functionaris voor Gegevensbescherming (FG) | • Toezicht en advisering op naleving privacy wetgeving<br>• Voorlichting privacy en stimuleren bewustwording<br>• Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens<br>• Waar nodig college van bestuur adviseren en ondersteunen<br>• Participeren in Werkgroep IBP<br>• Afwikkeling klachten en incidenten | • Privacyreglement.<br>• Zie ook hierboven, bij Werkgroep IBP. |

| | | | |
|---|---|---|---|
| | Eerstelijns verantwoordelijken voor:<br>Onderwijs, Facilitair, Financiën, ICT, Administratie en P&O | • Classificatie / risicoanalyse in samenwerking met de Werkgroep IBP en de FG.<br>• Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door CvB<br>• Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.<br>• Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren. | • Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister.<br>• Classificatie- en risicoanalyse documenten.<br><br>Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder:<br><br>• Toegangsmatrix diverse informatiesystemen en netwerk |
| **Uitvoerend (operationeel)** | Medewerkers Servicedesks ICT | • Incidentafhandeling (registreren en evalueren).<br>• Technisch en 1e aanspreekpunt voor IBP-incidenten, inclusief datalekken.<br>• Uitvoeren taken conform gegeven richtlijnen en procedures. | |
| | Leidinggevenden | • Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan.<br>• Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers.<br>• Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid.<br>• Implementeren IBP-maatregelen.<br>• periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;<br>• Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur. | Communiceren, informeren en toezien op naleving van o.a.:<br><br>• IBP in het algemeen<br>• Regels passend onderwijs<br>• Hoe omgaan met leerling dossiers<br>• Wie mogen wat zien<br>• Gedragscode<br>• Omgaan met sociale media |
| | Medewerkers (allen) | • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. | |

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

## Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende richtlijnen, procedures en protocollen; deels al aanwezig, deels in ontwikkeling en deels nog te ontwikkelen. De meeste van deze documenten zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

| **Documenten / bestanden:** | **Aandachtspunten / toelichting:** |
|---|---|
| Procedure toestemming gebruik beeldmateriaal | toestemmingsbrief |
| Procedure voor verwijderen van gegevens | bewaartermijnen |
| Privacyverklaring | communicatie aan betrokkenen over verwerking van hun gegevens |
| Procesbeschrijving rechten betrokkenen | proces rondom aanvragen van betrokkenen |
| Privacyreglement | Beschrijving rechten betrokkenen (leerlingen, ouders, medewerkers) |
| Autorisatiematrix | wie mogen gegevens inzien, bewerken enz. |
| Afspraken gebruik sociale media | |
| Procedure rondom voorlichting & training medewerkers | bewustzijn creëren |
| Protocol Cameratoezicht | |
| Responsible disclosure | verantwoord melden van aangetroffen beveiligingslekken |
| Gedragscode ICT en internetgebruik, Acceptable use policy | verantwoord gebruik bedrijfsmiddelen |
| Procedure rondom uitwisselen gegevens | passend onderwijs, leerling dossiers, leerplicht enz |
| Protocol melden datalekken / Registratie beveiligingsincidenten | |
| Verwerkingsregister (bestand) | Actuele registratie van alle verwerkingen (schoolprocessen) en de persoonsgegevens die daarbij verwerkt worden |
| Verwerkersovereenkomsten | Vastgelegde beveiligings- en privacy-afspraken met verwerkers (leveranciers) |
| Risicoanalyse / Procedure gegevensbeschermingseffectbeoordeling (“DPIA”) | Risico’s t.a.v. privacy in kaart brengen bij bestaande en nieuwe verwerkingen |
| Functionaris voor Gegevensbescherming | aanwijzing, communicatie hierover richting medewerkers, reglement |

## Bijlage 2: Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBP binnen Stichting Scala en Coenecoop op drie niveaus wordt georganiseerd.

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

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden binnen Scala en Coenecoop voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen. Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

### Richtinggevend

**Eindverantwoordelijke**
Het college van bestuur is als bevoegd gezag eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd.

### Sturend

**De Werkgroep voor IBP-beleid** is een rol op sturend niveau. Zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het college van bestuur), bewaakt een goede uitvoering van het IBP-beleid en stuurt waar nodig bij. Zij is verder verantwoordelijk voor:

- Het IBP-beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit van IBP bewaken binnen Scala en Coenecoop.
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De organisatie van ICT en informatiebeveiliging binnen Scala en Coenecoop

**Functionaris voor Gegevensbescherming (FG)**
De FG houdt binnen Stichting Scala en Coenecoop toezicht op de toepassing en naleving van de AVG en adviseert daarover. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP en het (ondersteunen bij) de afhandeling van datalek-incidenten. Hij adviseert over privacy-aangelegenheden, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het college van bestuur). Daarnaast werkt hij nauw samen met de Werkgroep IBP. De FG is ook de 2e lijns contactpersoon voor klachten en vragen van betrokkenen.

**Servicedesks ICT**
Zijn verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen de aangesloten scholen van Stichting Scala en Coenecoop. De Servicedesks ICT zijn ook verantwoordelijk voor het afhandelen van informatiebeveiligingsincidenten; in geval van datalekken in samenwerking met de FG.

**Eerstelijns verantwoordelijken**
Binnen de school zijn er verschillende domeinen en afdelingen, zoals onderwijs, ICT, personeel (P&O), leerlingadministratie, facilitaire- en financiële zaken etcetera. Op elk van deze domeinen en afdelingen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

De afdelingsleiders zijn tevens verantwoordelijk voor het voorkomen dat personen ten onrechte (te ruime) toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben afdelingsleiders de volgende specifieke taken:

- Samen met de directieverantwoordelijke voor IBP-beleid stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

## Uitvoerend

**Servicedesks ICT**
De Servicedesks ICT vormen op de aangesloten scholen een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers en het meldpunt voor beveiligingsincidenten en datalekken.

**Applicatie of functioneel beheerder**
In beginsel heeft ieder softwarepakket of (web-)applicatie dat gebruikt wordt binnen Stichting Scala en Coenecoop een functioneel beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De functioneel beheerder wordt vanuit de afdelingsleiders voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

**Medewerkers (allen)**
Alle medewerkers dragen verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in protocollen voor het gebruik van ICT-middelen en in de privacy gedragsregels van Stichting Scala en Coenecoop, zoals hiervoor geformuleerd onder 4.1. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.
Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van informatiebeveiligingsincidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR)

**Leidinggevende**
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering binnen Stichting Scala en Coenecoop. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn/haar medewerkers op de hoogte zijn van het IBP-beleid;
- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen

etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan hierbij ondersteund worden door de Werkgroep IBP en/of geadviseerd worden door de FG.