Informatiebeveiligings- en privacybeleid (IBP)

Besproken DB PO	26 september 2023
Besproken DB VO	6 oktober 2023
Vastgesteld CvB	9 oktober 2023
Ingestemd GMR PO	20 december 2023
Ingestemd MR VO	25 oktober 2023

Inhoudsopgave

1 Inleiding 3

1.1 Informatiebeveiliging en privacy (IBP) 3

2 Doel en reikwijdte 4

3 Uitgangspunten 5

3.1 Privacy 5

4 Wet- en regelgeving 7

5 Organisatie 8

5.1 Richtinggevend 8

5.2 Sturend 8

5.3 Uitvoerend 9

6 Controle en rapportage 9

6.1 Voorlichting en bewustzijn 10

6.2 Classificatie en risicoanalyse 10

6.3 Incidenten en datalekken 10

6.4 Controle, naleving en sancties 10

6.5 Logging en monitoring 11

Bijlage 1: Tabel IBP rollen en taken 12

Bijlage 2: Lijst ondersteunende richtlijnen en procedures 15

1 Inleiding

Informatie en ICT zijn noodzakelijk in de ondersteuning van het onderwijs. Omdat we met persoonsgegevens (van onszelf, leerlingen en anderen) werken, is de Algemene Verordening Gegevensbescherming (AVG) daarop van toepassing.

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door onder andere 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.

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

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.

Om dit structureel op te pakken is het noodzakelijk dat er duidelijk gemaakt wordt waar het om gaat, dat er een doel gesteld wordt en de manier waarop we dit doel willen gaan bereiken, expliciteren.

1.1 Informatiebeveiliging en privacy (IBP)

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

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:

Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

Uit het voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit beleid vormt de basis om IBP

binnen SCO te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

2 Doel en reikwijdte

IBP heeft de volgende doelen:

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

Dit beleid is een leidraad voor alle medewerkers, leerlingen en direct betrokkenen binnen SCO en is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (onder anderen medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en SCO voldoet aan relevante wet- en regelgeving. Het is van toepassing op de gehele organisatie, waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.

IBP heeft raakvlakken met andere beleidsgebieden, te weten:

- algemeen veiligheids- en beveiligingsbeleid, met als aandachtsgebieden bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen;
- ICT-beleid, met als aandachtsgebieden de aanschaf, het beheer en gebruik van ICT;
- personeels- en organisatiebeleid. met als aandachtsgebieden werving- en selectietrajecten, in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.

Dit beleid maakt duidelijk waar de verantwoordelijkheden rondom IBP zijn belegd.

3 Uitgangspunten

De belangrijkste beleidsuitgangspunten bij SCO zijn:

- Het IBP-beleid dient 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;
- SCO is eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt;
- SCO maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over IBP;
- IBP is een continu proces, waarbij regelmatig 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;
- Bij SCO is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen;
- SCO legt alle verwerkingen van persoonsgegevens vast in een verwerkingsregister;
- SCO kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen voorafgaand naar de impact hiervan op IBP, zodat tijdig de juiste maatregelen kunnen worden genomen;
- SCO neemt passende technische (beveiligings)maatregelen om persoonsgegevens en overige data te beschermen tegen risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren;
- SCO zal alle beveiligingsincidenten en datalekken vastleggen en volgens een vast protocol afhandelen. Indien nodig, in overleg met de functionaris gegevensbescherming wordt er melding gedaan bij de Autoriteit Persoonsgegevens en de betrokkenen.

3.1 Privacy

SCO hanteert vijf vuistregels, de wettelijke beginselen (art.5 AVG) voor het omgaan met persoonsgegevens:

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/verzorgers 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.

4 Wet- en regelgeving

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

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs;
- Wet goed onderwijs en goed bestuur PO/VO;
- Algemene Verordening Gegevensbescherming (AVG) (i.p.v. Wet bescherming persoonsgegevens v.a. 25 mei 2018);
- Archiefwet;
- Leerplichtwet;
- Auteurswet;
- Wetboek van Strafrecht;
- Wet op het onderwijstoezicht.

Het normenkader funderend onderwijs is leidend voor de te nemen beveiligingsmaatregelen.

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

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 2 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in het verwerkingsregister.

5 Organisatie

Dit hoofdstuk beschrijft hoe IBP binnen SCO 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.

5.1 Richtinggevend

Eindverantwoordelijke

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

5.2 Sturend

Rol bestuursbureau

De directeur bedrijfsvoering heeft een rol op sturend niveau, geeft terugkoppeling en advies aan het CvB en stuurt de mensen aan op de uitvoerende laag. De directeur bedrijfsvoering moet:

- het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling;
- de uniformiteit bewaken binnen SCO;
- het aanspreekpunt zijn voor incidenten op het gebied van IBP;
- de verdere afhandeling van incidenten binnen SCO coördineren.

Domeinverantwoordelijkheid/proceseigenaar

Binnen SCO 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 binnen SCO hebben in deze een voorbeeldrol ten opzichte van hun medewerkers.

Functionaris voor gegevensbescherming

De functionaris voor gegevensbescherming (verder te noemen FG) houdt binnen SCO toezicht op de toepassing en naleving van de privacywetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. De FG heeft regelmatig overleg met de directeur bedrijfsvoering. De FG is meestal ook contactpersoon voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.

SCO heeft de rol van FG belegd bij Privacy op School.

5.3 Uitvoerend

De hieronder genoemde functies, betreffen geen opzichzelfstaande functies maar vallen binnen het takenbeleid.

Databeveiliger

De databeveiliger vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging. Binnen het VO locaties CLD betreft dit de systeembeheerders van de ICT-helpdesk. Binnen het PO en VO (locatie sc Delfland) betreft dit de interne contactpersoon die het contact verzorgt met de externe beheerder.

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 taken uit. Te denken valt bijvoorbeeld aan het functionele beheer van diverse applicaties, websites en schoolgidsen.

Leidinggevende

Naleving van het IBP-beleid 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 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.

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

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in de ‘Gedragscode t.a.v. verantwoord gebruik bedrijfsmiddelen door medewerkers’. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Aan medewerkers wordt onder andere gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van incidenten, datalekken, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de GMR PO of MR VO).

6 Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuursbureau 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 SCO een jaarlijkse planning- en controlcyclus voor IBP. Dit is een periodiek evaluatieproces waarmee de inhoud van het IBP-beleid wordt getoetst.

6.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van IBP uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste factor. Daarom wordt bij SCO 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 de directies binnen SCO, databeveiligers, de functioneel beheerders, met het College van Bestuur als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse

Bij SCO 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 zijn voor de informatievoorziening.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact (DPIA) van de ontwikkelingen en de beoogde verwerkingen op IBP, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ICT-)projecten wordt rekening gehouden met IBP.

6.3 Incidenten en datalekken

Alle medewerkers die een beveiligingsincident of datalek vermoeden, dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in het protocol beveiligingsincidenten en datalekken. De afhandeling van deze incidenten gaat volgens een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld via de link op intranet of per mail naar meldpuntdatalekken@scodelft.nl.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig zullen aanvullende passende beleidsmaatregelen genomen worden.

6.4 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 SCO wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een organisatiebrede gedragscode

(integriteitscode en gedragscode verantwoord gebruik bedrijfsmiddelen), met periodieke bewustwordingscampagnes, et cetera.

Voor toezicht op de naleving van de AVG vervult de FG een belangrijke rol. De FG wordt aangesteld door het CvB, 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 tekortschieten, dan kan SCO de betrokken verantwoordelijke medewerker een sanctie opleggen, binnen de kaders van de cao en de wettelijke mogelijkheden.

Bij SCO is het melden van beveiligingsincidenten en datalekken vastgelegd in het protocol beveiligingsincidenten en datalekken.

6.5 Logging en monitoring

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

Bijlage 1: Tabel IBP rollen en taken

Niveau	**Wie?** **Rollen**	**Hoe?** **Verantwoordelijkheid / taken**	**Wat?** **Realiseren / vastleggen**
Richtinggevend **(strategisch)**	CvB	• Eindverantwoordelijk • IBP-beleidsvorming, vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Verantwoordelijk voor het accepteren van eventuele restrisico's • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacybeleid • Baseline basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend **(tactisch)**	Privacy-officer: Directeur bedrijfsvoering (eindverantwoordelijk) en beleidsmedewerker bedrijfsvoering	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en -controle • Adviseert bestuur/CvB/directie 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 • Afwikkeling klachten en incidenten • Het treffen van mitigerende maatregelen	Processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Bijhouden verwerkingsregister • Brief toestemming gebruik foto's en video • Bijhouden incidentenregister • Opstellen informatie documentatie richting leerlingen, ouders/verzorgers • Security awareness-activiteiten • Sociale media beleid • Integriteitscode • Gedragscode t.a.v. verantwoord gebruik bedrijfsmiddelen

	Functionaris voor gegevens-bescherming (FG)	• Toezicht op naleving privacywetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Toezicht op afwikkeling klachten en incidenten	• Privacyreglement, • Procedure afhandeling IBP-incident • Inrichten meldpunt datalekken
Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
	Domeinverant-woordelijke/ Proceseigenaren waaronder: ICT, personeel en administratie	• **Classificatie / risicoanalyse** in samenwerking met Manager IBP (Informatiemanager / verantwoordelijke IBP / data-beveiliger) • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie • 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 • Samen met functioneel beheer en ICT-beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leverancierslijst) • Classificatie- en risicoanalyse documenten Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
Uitvoerend **(operationeel)**	Databeveiliger	• Incidentafhandeling (registreren en evalueren)	

	Functioneel beheerder Medewerker	• Technisch aanspreekpunt voor IBP-incidenten • Uitvoeren taken conform gegeven richtlijnen en procedures • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden	Communiceren, informeren en toezien op naleving van veilig gebruik van persoonsgegevens
Niveau	**Wie?** **Rollen**	**Hoe?** **Verantwoordelijkheid / taken**	**Wat?** **Realiseren / vastleggen**
	Dagelijkse leiding / leidinggevende / directie	• 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	• IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken

Bijlage 2: Lijst ondersteunende richtlijnen en procedures

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

Integriteitscode

Gedragscode t.a.v. verantwoord gebruik bedrijfsmiddelen (2024)

Protocol beveiligingsincidenten en datalekken

Protocol klachten AVG, rechten van betrokkenen

Privacyreglement verwerking persoonsgegevens