GOOISE SCHOLEN FEDERATIE

Informatiebeveiligings- en privacybeleid

Gooise Scholen Federatie

Vastgesteld door College van Bestuur op 20 november 2017

1. Inleiding

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

De informatie en ICT van de GSF worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan worden bedreigd door bijvoorbeeld een cyber-aanval, een ramp (bijv. overstroming of brand) of een menselijke vergissing. Het niet beschikbaar zijn van ICT, incorrecte administraties en het uitlekken van gegevens kan belemmeringen geven bij het geven van onderwijs en het vertrouwen schaden van personeel, ouders en leerlingen in onze school.

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, een doel stellen en de manier waarop we dit doel willen bereiken. Door te werken volgens de PDCA-cyclus, zullen we stap voor stap dichter bij het vastgestelde doel komen.

1.1. Informatiebeveiliging en privacy

Informatiebeveiliging is een proces voor het beschermen van de GSF 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 diegenen 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. Achtergrond

In april 2015 hebben de PO-Raad, de VO-raad, de Groep Educatieve Uitgeverijen (GEU), de Vereniging Digitale Onderwijs Dienstverleners (vDOD) en de leden van de sectie Educatief van de Koninklijke Boekverkopersbond het convenant 'Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen' ondertekend. Het convenant regelt onder meer dat de scholen, en niet de aanbieders van digitale onderwijsmiddelen, de regie hebben op wat er gebeurt met de gegevens die worden verwerkt bij het gebruik van digitale onderwijsmiddelen. Ook is in het convenant opgenomen dat scholen, onder meer op basis van gegevens van aanbieders, ouders en leerlingen informeren over het gebruik van persoonsgegevens en over hoe ouders en leerlingen gebruik kunnen maken van hun rechten zoals inzage en correctie. Het convenant concretiseert hiermee de naleving van de verplichtingen van scholen en hun leveranciers die uit

de Wet bescherming persoonsgegevens (Wbp) voortvloeien.
De ontwikkelingen in de ICT gaan snel en ook de (Europese) privacywetgeving is in beweging. Privacy- en informatiebeveiliging blijven daarom voortdurend aandacht vragen. Zorgvuldig omgaan met persoonsgegevens vraagt om een goede beveiliging. Scholen zijn verplicht om persoonsgegevens te beveiligen tegen risico's zoals verlies, onbevoegde toegang, vernietiging, gebruik, wijziging of openbaarmaking van de gegevens.

Sinds 1 januari 2016 is de Wet bescherming persoonsgegevens (Wbp) gewijzigd. De meest besproken wijziging is daarbij de invoering van de meldplicht datalekken, waarbij de boetebevoegdheden van de Autoriteit persoonsgegevens aanzienlijk zijn uitgebreid. Op 25 mei 2018 treedt de nieuwe Europese Algemene Verordening Gegevensbescherming (AVG) in werking. Deze Europese AVG vervangt de huidige Nederlandse Wet bescherming persoonsgegevens (Wbp) en heeft grote implicaties voor zowel de private als publieke sector.

1.3. Rol Kennisnet

Kennisnet heeft met eigen expertise en veel bezoeken aan scholen bekeken wat werkt en wat veelvoorkomende uitdagingen zijn. Dat is dan ook het uitgangspunt geweest voor de PO-Raad, VO-raad en Kennisnet om een aanpak te ontwikkelen die scholen helpt met het op eenvoudige en praktische wijze organiseren van informatiebeveiliging en privacy (IBP). De GSF maakt gebruik van deze aanpak en heeft de beleidsdocumenten opgesteld met behulp van deze aanpak.

2. Doel en reikwijdte

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 GSF-scholen. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen in de GSF. Het is van toepassing op de hele organisatie, 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;
- ICT-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.

3. Uitgangspunten

De belangrijkste beleidsuitgangspunten 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 GSF is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt;
- De GSF maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy;
- Informatiebeveiliging en Privacy zijn 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.

3.1. Privacy

De GSF 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; Het staat 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.

4. Wet- en regelgeving

4.1. Wet bescherming persoonsgegevens

Zeer veel organisaties gebruiken persoonsgegevens en wisselen deze uit. De belangrijkste regels voor de omgang met persoonsgegevens in Nederland zijn vastgelegd in de Wet bescherming persoonsgegevens.
De Wet bescherming persoonsgegevens (Wbp) is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens. De Wbp is sinds 1 september 2001 van kracht.
De Wbp regelt ook de taken en bevoegdheden van de Autoriteit Persoonsgegevens als toezichthouder op deze wet en andere wet- en regelgeving voor de verwerking van persoonsgegevens.

Belangrijkste bepalingen Wbp
De belangrijkste bepalingen uit de Wbp over het rechtmatig omgaan met persoonsgegevens zijn als volgt samen te vatten:

- Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt;
- Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. En vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn;
- Degene van wie persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verantwoordelijke) en van het doel van de gegevensverwerking;
- De gegevensverwerking moeten op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

4.2. Algemene Verordening Gegevensbescherming

Per 25 mei 2018 is de algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum nog maar één privacywet geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.
De Europese privacyrichtlijn werd vastgesteld toen internet nog in de kinderschoenen stond. Daarom is de Europese privacywetgeving de afgelopen jaren herzien.

De AVG zorgt onder meer voor:

- versterking en uitbreiding van privacyrechten
- meer verantwoordelijkheden voor organisaties
- dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders.

4.3. Overzicht relevante wetgeving

De volgende relevante wet- en regelgeving zijn van toepassing op het informatiebeveiligings- en privacybeleid:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- 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.

5. Organisatie

Dit hoofdstuk beschrijft hoe IBP bij de GSF 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. In het kader van de nieuwe Algemene Verordening Gegevensbescherming (AVG), is voor alle organisaties de aanwijzing van een interne Functionaris Gegevensbescherming een verplichting.

5.1. Richtinggevend

Eindverantwoordelijke

Het College van Bestuur 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 hen geëvalueerd. Binnen het CvB is het lid CvB verantwoordelijk voor IBP.

5.2. Sturend

Functionaris voor Gegevensbescherming

De Functionaris voor gegevensbescherming (FG) houdt 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. FG heeft regelmatig overleg met manager IBP. De FG is meestal ook contactpersoon en voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.

<u>Taken</u>

De taken van de Functionaris voor Gegevensbescherming omvatten onder meer:

Beleidsmatig:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling;
- Het ontwikkelen van interne privacygerelateerde regelingen;
- Input leveren bij het opstellen of aanpassen van een gedragscode;
- Awareness op het gebied van privacy onderhouden;
- Overleg voeren met de privacyverantwoordelijken van de scholen.

Controlematig:

- Toezicht houden op de naleving van wet- en regelgeving, alsmede op de naleving van de organisatie afspraken op privacy gebied;
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy;
- Coördineren van het proces van datalekken;

- Contact onderhouden met extern contact: privacycheck met extern;
- Behandeling van vragen en klachten van binnen en buiten de organisatie;
- Verzamelen van inventarisaties van gegevensverwerkingen;
- Het bijhouden van meldingen van gegevensverwerkingen/datalekken;
- Gevraagd en ongevraagd advies uit binnen de eigen organisatie over privacy aangelegenheden en voorstellen doen om privacyrisico's te beperken.

Een Functionaris voor Gegevensbescherming heeft geen formele sanctiebevoegdheden, maar hij/zij moet wel bevoegd zijn om ruimtes te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen. De FG en de privacyverantwoordelijken (zie hieronder) moeten in onafhankelijkheid hun werkzaamheden kunnen verrichten binnen een organisatie.

privacyverantwoordelijke (per school)
Op iedere school is een privacyverantwoordelijke aanwezig, die aanspreekpunt is voor alle privacyzaken en beveiligingsincidenten op een school. Deze rol maakt onderdeel uit van de directie portefeuille. De privacyverantwoordelijke heeft regelmatig contact met de FG en beoordeelt in geval van beveiligingsincidenten of geëscaleerd moet worden naar de ICT-privacycoördinator volgens de procedure 'Meldplicht datalekken'.

Taken
- Zorgdragen voor de naleving van wet en regelgeving, alsmede de schoolafspraken op privacygebied;
- Gevraagd en ongevraagd advies uiten binnen de eigen organisatie over privacy aangelegenheden en voorstellen doen om privacyrisico's te beperken;
- Behandeling van vragen en klachten van binnen en buiten de organisatie;
- Aanspreekpunt bij beveiligingsincidenten en mogelijk escaleren volgens de procedure datalekken;
- Bijdragen aan het ontwikkelen van interne privacygerelateerde regelingen bovenschool;
- Input leveren bij het opstellen of aanpassen van een gedragscode;
- Bevorderen van de awareness op de scholen.

5.3. Uitvoerend

ICT-privacycoördinator
De ICT-privacycoördinator vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging.
Taken
- Adviseren over technologie en beveiliging, waaronder voorlichting over privacy;
- Verantwoordelijk voor het opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende informatie (beveiligingsplannen);
- Initiëren of laten uitvoeren van periodieke beveiligingsaudits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses;
- Coördineren en adviseren bij beveiligingsincidenten en zo nodig optreden bij calamiteiten;
- Op de hoogte blijven van ontwikkelingen op het gebied van informatiebeveiliging en zo nodig met voorstellen komen voor aanvullingen of verbeteringen van producten, methodieken of werkwijzen met betrekking tot de informatiebeveiliging;
- Het formele, en bij iedereen in de organisatie bekende, aanspreekpunt voor „informatiebeveiligingszaken"

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 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 de MR)

Leidinggevenden
Naleving van het informatiebeveiligingsbeleid 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.;
- Als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de Functionaris voor Gegevensbescherming.

6. Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door het CvB. 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 GSF 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.

6.1. 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 GSF 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 Functionaris voor Gegevensbescherming, de privacyverantwoordelijke per school en de ICT-privacycoördinator met het College van Bestuur als eindverantwoordelijke.

6.2. Classificatie en risicoanalyse

Alle informatie heeft 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.

6.3. Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij ICT Support. De afhandeling van deze incidenten volgt een gestructureerd proces, die 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 IBP proces. 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 instellingsbrede gedragscode, met periodieke bewustwordingscampagnes. Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de FG een belangrijke rol. Mocht de naleving ernstig tekort schieten, dan kan de GSF de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol.

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 • evalueren toepassing en werking IBP-beleid op basis van rapportages • organisatie IBP inrichten	• informatiebeveiligings- en privacybeleid • basismaatregelen • privacyreglement vaststellen
Sturend (tactisch)	Functionaris voor Gegevens-bescherming beleidsmatig	• 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	Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • protocol beveiligingsincidenten en datalekken • bewerkersovereenkomsten 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 Gegevens-bescherming controlematig	• toezicht op naleving privacywetgeving • richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • afwikkeling klachten en incidenten • coördinatie proces datalekken	• privacyreglement, • procedure IBP-incident afhandeling • inrichten meldpunt datalekken
	Domeinver-antwoordelijke - ICT - p&o - financiën / administratie	• classificatie / risicoanalyse (in samenwerking met Manager IBP); • toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door *CvB* • *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 (leveranciers lijst) • classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • toegangsmatrix diverse informatiesystemen en netwerk

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Uitvoerend (operationeel)	ICT privacy-coördinator	● adviseren over en vernieuwen van technologie en beveiliging ● initiëren van periodieke beveiligingaudits ● incidentafhandeling (registreren en evalueren). ● technisch aanspreekpunt voor IBP-incidenten.	
	Medewerker	● verantwoordelijk omgaan met IBP bij dagelijkse werkzaamheden.	
	Dagelijkse leiding en privacy verantwoordelijke	● 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.: ● IBP in het algemeen ● regels passend onderwijs ● hoe omgaan met leerling dossiers ● wie mag wat zien ● gedragscode ● omgaan met sociale media ● mediawijs maken