Privacy en informatiebeveiligingsbeleid (versie 1.0)

De Waterlelie

Opdrachtgever	R. Veldhuijzen van Zanten (portefeuillehouder IBP)
Opdrachtnemer	S. Zijlstra (Privacy Officer)
Document	Beleid Informatiebeveiliging & Privacy
Auteur	S. Zijlstra

Versie	Datum	Opmerkingen
V.01	12-12-2022	Concept
V.02	12-01-2023	Definitief
V.02	20-06-2023	Akkoord MR

Inhoudsopgave

Inleiding

Dit document betreft de invulling van het beleid Informatiebeveiliging & Privacy van De Waterlelie.

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen. Privacy en bescherming van persoonsgegevens maakt daar een belangrijk onderdeel van uit.

School De Waterlelie valt onder het bestuur van SEIN (Stichting Epilepsie Instellingen Nederland)

Door de directie van de Waterlelie is besloten om een eigen IBP-beleid voor personeel en leerlingen op te stellen. SEIN bedient andere doelgroepen (patiënten en cliënten) waardoor er een groot verschil is in de verwerking van gegevens van leerlingen en die van cliënten/ patiënten. Daarnaast gelden er in het onderwijs andere wet- en regelgevingen. De Waterlelie volgt op hoofdlijnen het beleid van SEIN. In dit document wordt hier uitleg aan gegeven.

1. Het belang van informatiebeveiliging en privacy

Privacy is een grondrecht, het betreft het recht op bescherming van de persoonlijke levenssfeer.

Informatie is één van de belangrijkste bedrijfsmiddelen van De Waterlelie. Toegankelijke en betrouwbare informatie en borging van de privacy zijn essentieel voor een onderwijsorganisatie als De Waterlelie die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan zijn leerlingen. De bescherming van waardevolle en/of vertrouwelijke informatie is hetgeen waar het uiteinde-

lijk om gaat. Hoe waardevoller en vertrouwelijker de informatie is, hoe meer maatregelen er getroffen worden om gegevens maximaal te beschermen tegen inbreuk. Het onderwijs is in toenemende mate afhankelijk van digitale informatie. Dit brengt nieuwe kwetsbaarheden en risico's met zich mee. Om inzicht en grip te houden op de risico's en de informatiebeveiliging en privacy (afgekort tot IBP) op orde te brengen is een is een IBP-beleid noodzakelijk. Met een IBP beleid blijft om mogelijke gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

Het IBP beleid 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.

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 school. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

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 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.

2.3. Vervlechting informatiebeveiliging en privacy

Uit 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, verder te benoemen als IBP-beleid, vormt de basis op informatiebeveiliging en privacy binnen De Waterlelie te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3. Doel en reikwijdte

3.1. Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- ➢ Het garanderen van de privacy van alle betrokkenen waarvan De Waterlelie persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- ➢ Het voldoen aan Verlies van Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie vergroot de kans op Incidenten en Datalekken;
- ➢ Het voldoen aan relevante wet- en regelgeving en randvoorwaardelijke eisen van privacy en informatiebeveiliging;
- ➢ Het beschermen en versterken van de reputatie op het gebied van privacy en informatiebeveiliging;
- ➢ Het stimuleren van een verantwoordelijke en transparante organisatiecultuur waarin Incidenten en datalekken tijdig ontdekt, gemeld en afgehandeld worden;
- ➢ Het zorg dragen dat de medewerkers adequaat zijn getraind om de aan haar toegewezen taken en -verantwoordelijkheden privacy veilig uit te kunnen voeren;
- ➢ Het zorg dragen voor bescherming van de informatie en haar onderliggende systemen tegen (cyber)criminaliteit;
- ➢ Het zorg dragen dat kwetsbaarheden worden geïdentificeerd en worden weggenomen;

De Waterlelie streeft ernaar om ‘in control’ te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent dat de organisatie weet welke maatregelen genomen zijn en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn en als laatste, dat dit geheel verankerd is in de PDCA-cyclus voor informatiebeveiliging.

3.2. Reikwijdte

Informatiebeveiliging en privacy is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, USB, beeldscherm etc.) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen. Het IBP-beleid binnen de Waterlelie geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/ outsourcing). Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische en niet-geautomatiseerde verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van de Waterlelie evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen.

4. Beleid – Hoe doen we dat?

De Waterlelie hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van De Waterlelie neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.

2. De Waterlelie voldoet aan alle relevante wet- en regelgeving.

3. Bij De Waterlelie is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van De Waterlelie om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.

4. De Waterlelie zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.

5. De Waterlelie legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. De Waterlelie voldoet hiermee aan de documentatieplicht.

6. Binnen De Waterlelie is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.

7. De Waterlelie 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. De Waterlelie verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich ‘fatsoenlijk’ gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. De Waterlelie heeft een gedragscode geformuleerd. Medewerkers krijgen via verschillende kanalen informatie over het verwantwoord omgaan met van informatie. Het bewustzijn van medewerkers wordt voortdurend aangescherpt, zodat de kennis van risico’s wordt verhoogd en veilig en verantwoord en gedrag aangemoedigd wordt. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers en leerlingen. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke Privacy Officer met het bestuur als eindverantwoordelijke en de FG als toezichthouder op naleving.

8. Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen 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 betrouwbaarheidsaspecten die van belang zijn.

9. Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy door middel van een DPIA (data protection privacy assesment) . Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

10. De aanpak van informatiebeveiliging en privacy is ‘risk based’. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de ISO 27001, de AVG en binnen de Waterlelie vastge-

stelde referentiewaarden. Indien een systeem meer maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd. Daartoe inventariseert de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar: risico=kans x impact.

11. De Waterlelie sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.

12. Informatiebeveiliging en privacy is bij De Waterlelie een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is. 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.

13. De Waterlelie neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.

14. De Waterlelie legt alle beveiligingsincidenten vast en volgt het datalekken protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen hier een melding van te maken. Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5. Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

5.1. Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2017) is leidend voor de te nemen beveiligingsmaatregelen. De Waterlelie verwerkt ook gezondheidsgegevens, voor deze gegevens worden de eisen vanuit de NEN7510/NEN7512 en NEN7513, waar mogelijk, toegepast.

5.2. Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

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 manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.

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 staan tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Opslagbeperking:** Indien Persoonsgegevens niet meer noodzakelijk zijn (of de wettelijke bewaartermijn is verstreken) dient vernietiging plaats te vinden. De Waterlelie geeft toepassing aan het principe van opslagbeperking door een bewaartermijnenbeleid te voeren en te handhaven, waarbij Persoonsgegevens niet langer worden bewaard dan strikt noodzakelijk is voor het beoogde doel. Bij het langer bewaren van persoonsgegevens wordt dit in een vorm bewaard die het mogelijk maakt de dat een betrokkene niet langer te identificeren is.

5. **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 betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

6. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

7. **Privacy by Design & Privacy by Default:** De AVG vereist dat reeds bij het ontwerp van (nieuwe) producten/diensten rekening wordt gehouden met de bescherming van Persoonsgegevens (‘privacy by design’ oftewel: ‘gegevensbescherming door ontwerp’) en dat in relatie tot Betrokkenen privacy ook als ‘standaardinstelling’ moet zijn doorgevoerd (‘privacy by default’ of ‘gegevensbescherming door standaardinstellingen).

De Waterlelie streeft ernaar haar applicaties en informatievoorziening standaard in richten op de meest privacy vriendelijke wijze en houdt hiermee ook rekening bij de selectie van (nieuwe) leveranciers / Verwerkers. Concreet houdt dit bijvoorbeeld in dat indien ‘toestemming’ wordt gevraagd, er altijd sprake zal zijn van een actieve handeling (‘opt-in’ in plaats van ‘opt-out’), dat applicaties standaard zo weinig mogelijk Persoonsgegevens dienen te verwerken (bv. geen onnodige locatiegegevens), en dat Betrokkenen altijd een

5.3. Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 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 een dataregister.

5.4 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 instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan De Waterlelie de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.6 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt ervoor 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. Mogelijke ´trigger´ situaties waarvan verwacht kan worden dat dossiers van leerlingen of medewerkers tot ongeoorloofd inzage kan leiden worden door het management gesignaleerd waarop er toegangscontrole plaatsvindt. Daarnaast worden er jaarlijks steekproefsgewijs toegangscontroles op de leerling dossiers uitgevoerd en gerapporteerd.

6. Organisatie - Wie doet wat?

6.1. 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 spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij De Waterlelie.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid/ taken	Wat Realiseren/ vastleggen
Richtinggevend **(strategisch)**	Directeur	• 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 privacy beleid • Baseline/ basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend **(tactisch)**	Privacy officer	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, • 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. • **Classificatie / risicoanalyse** in samenwerking met verantwoordelijke IBP en FAB (functioneel applicatie beheer) • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie. • Voorlichting privacy en stimuleren bewustwording	Processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Security awareness activiteiten • Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van infor-
	FG	• Toezicht op naleving AVG-wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • Procedure IBP-incident afhandeling

	Proceseigenaren waaronder o.a.: ICT, HRM / P&O, onderwijs, financiën,	• Samen met functioneel beheer en ICT-beheer erop 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); input dataregister • Classificatie- en risicoanalyse documenten.
Uitvoerend **(operationeel)**	Verantwoordelijke IBP	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten.	• Gedragscode medewerkers en leerlingen. • Opstellen informatie documentatie richting leerlingen, ouders/ verzorgers. • Gedragscode social media, ict en inter netgebruik.
	Functioneel en/ of applicatie beheerder	• Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; ervoor 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.	• Toegangsmatrix diverse informatiesystemen en netwerk • Aanleveren rapportage controle van de logging.
	Medewerker	• 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 mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken
	Dagelijkse leiding/ leidinggeven-		

IBP team:

Een IBP-team wordt organisatie breed zowel preventief als curatief benoemd voor informatiebeveiliging en privacy incidenten. De leden van het IBP-team zijn benoemd door de eindverantwoordelijke en handelen in diens opdracht.

Het IBP-team van De Waterlelie heeft de volgende opdracht:

- Het signaleren en registreren van alle privacy verzoeken, beveiligingsincidenten en datalekken. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot incidenten hebben geleid of waardoor de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het leveren van managementrapportages en verbetervoorstellen aan de domeinverantwoordelijke/proceseigenaren over de beveiligingsincidenten en verzoeken tot uitoefening privacy rechten van de betrokkenen.

Bij een calamiteit kan het IBP-team terstond bij elkaar worden geroepen op initiatief van de verantwoordelijke IBP, in opdracht van het De Waterlelie. Het doel hiervan is om de continuïteit van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

- Datalek;
- Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
- Natuurrampen (brand, overstroming, storm, etc.).

Het IBP-team bij De Waterlelie behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.

De werkzaamheden van het IBP-team bij De Waterlelie is gedocumenteerd en door de eindverantwoordelijke bekrachtigd.

Bijlage 1: Ondersteunende richtlijnen en procedures

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

Documenten:	Aandachtspunten:
Informatiebeveilgingsbeleid	
Procedure toestemming gebruik beeldmateriaal	(toestemmingsbrief)
Bewaar en vernietigingsbeleid	(bewaartermijnen)

Procesbeschrijving rechten betrokkenen	(proces rondom aanvragen van betrokkenen)
Autorisatiematrix	(wie mogen gegevens inzien, bewerken enz.)
Gedragsprotocol sociale media	(voor zowel leerlingen als medewerkers)
Communicatieplan IBP	(bewustzijn creëren)
Wachtwoordbeleid	
Toegangscontrole beleid	(fysieke en digitale toegang tot ruimtes en systemen)
Recovery plan	(wat te doen na een data inbreuk of verlies)

Verplicht vanuit de AVG:

Privacyverklaring	(transparantie naar betrokkenen over welke gegevens en hoe deze gegevens verwerkt worden, rechten van betrokkenen)
Procesbeschrijving melden datalekken	
Registratie beveiligingsincidenten	
Dataregister om te voldoen aan de registratieplicht	
Verwerkersovereenkomsten	(privacy bijlage beschikbaar stellen)
Procedure gegevensbeschermingseffectbeoordeling	(DPIA)
Risicoanalyse	