Informatiebeveiligings- en privacy beleid 2.0 van OVO Zaanstad

OPENBAAR VOORTGEZET ONDERWIJS ZAANSTAD

Bron: Kennisnet
Bewerkt door: Stichting OVO Zaanstad
Formele versie gericht op compliance

Expertise: IBP
Besluitvorming: AMO ter advisering op 15 december 2022
GMR ter instemming op 20 maart 2023
Vastgesteld door College van Bestuur op 28 maart 2023
Revisiedatum: 1 april 2025 (jaarlijks checken op actualiteit)

Inhoudsopgave

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.

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.

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 Stichting OVO Zaanstad (verder te noemen OVO Zaanstad) 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 waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan OVO Zaanstad persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (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. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en OVO Zaanstad voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen OVO Zaanstad geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (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 OVO Zaanstad waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan OVO Zaanstad persoonsgegevens verwerkt.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van OVO Zaanstad. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van OVO Zaanstad 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.

- IBP-beleid heeft binnen OVO Zaanstad 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
  - *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
  - *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

4 Beleid – Hoe doen we dat?

OVO Zaanstad hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van OVO Zaanstad 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. OVO Zaanstad voldoet aan alle relevante wet- en regelgeving.

3. Bij OVO Zaanstad 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 OVO Zaanstad 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 te alle tijden hun toestemming herzien.

4. OVO Zaanstad zal alle betrokkenen helder en actief informeren over de verwerkingen van 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 (het recht om OVO Zaanstad te vragen gegevens over te dragen) en profilering (het recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming).

5. OVO Zaanstad legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal dit up-to-date houden. OVO Zaanstad voldoet hiermee aan de documentatieplicht.

6. Binnen OVO Zaanstad 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. OVO Zaanstad 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.

8. OVO Zaanstad classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

9. OVO Zaanstad 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 verwerkt.

10. OVO Zaanstad 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. OVO Zaanstad heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij OVO Zaanstad een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. OVO Zaanstad kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. OVO Zaanstad 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.
    Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt OVO Zaanstad aanvullende afspraken vast over de technische maatregelen.

14. OVO Zaanstad zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen. Alle verantwoordelijken zijn op de juiste wijze geschoold.

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. Aanvullend heeft OVO Zaanstad eigen speerpunten opgenomen in haar beleid voor de komende vier jaar, zie paragraaf 5.10.

5.1 Relevante wet- en regelgeving

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

- Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) 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, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

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 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. **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.

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

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 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 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, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de bovenschoolse privacy-officer, de functionaris gegevensbescherming, en de security officer met het bestuur als eindverantwoordelijke.

5.5 Classificatie en risicoanalyse

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. Zie ook paragraaf 5.10.10.
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, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.6 Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit per ommegaande te melden aan de functionaris gegevensbescherming en/of de bovenschools privacy-officer.

Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister (op de teamssite van de privacy-medewerkers).

Elke school is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging. De incidenten worden geregistreerd volgens een standaard indeling, waardoor een objectieve vergelijking met incidenten bij andere instellingen mogelijk wordt. De incidenten worden afgehandeld en dienen als input voor de incidentrapportages, waarover in het operationeel overleg wordt gesproken. Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

Stichting OVO Zaanstad heeft een proces voor het melden en afhandelen van datalekken binnen de organisatie. De functionaris gegevensbescherming is de eigenaar van dit proces. Alle datalekken worden vanuit OVO Service afgehandeld. De afhandeling van informatiebeveiligingsincidenten vindt plaats door de (bovenschools) privacy-officer en schooldirectie dan wel CvB.

Een datalek met een grote impact wordt opgeschaald naar het crisisteam. Het college van bestuur heeft de leiding bij een datalek met een grote impact. De security officer wordt ingezet om onderzoek te doen naar de oorzaak wanneer er sprake is van een digitaal datalek.

5.7 Planning en controle

Dit IBP-beleid wordt jaarlijks gecheckt en zo nodig 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 OVO Zaanstad 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.

5.8 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, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de functionaris voor gegevensbescherming een belangrijke rol. De functionaris gegevensbescherming wordt aangesteld door het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De functionaris gegevensbescherming werkt via een door het bestuur vast te stellen reglement.

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

5.9 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt er voor 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.

5.10 Speerpunten beleid OVO Zaanstad

OVO Zaanstad zet de komende vier jaar in op de volgende speerpunten:

5.10.1 Privacyverklaring en Gedragscode

OVO Zaanstad wil dat iedereen die met de organisatie te maken heeft volledig geïnformeerd is over zijn rechten en/of plichten ten aanzien van de verwerking van (persoonlijke) informatie.

Daar waar het de rechten betreft, wordt er voor elk van de relevante doelgroepen een privacyverklaring opgesteld. Dat betekent dat er een separate privacyverklaring is voor ouders, leerlingen en medewerkers waarin OVO Zaanstad vermeldt op welke basis en hoe persoonlijke gegevens verwerkt worden. Ook vermeldt de verklaring hoe elk van de doelgroepen bezwaar kan aantekenen, of de te volgen procedure wanneer één van hen vermoedt dat er niet goed met de gegevens is omgesprongen.

Daar waar het plichten betreft, wordt er een gedragscode opgesteld. Er is een gedragscode voor zowel medewerkers als leerlingen. De gedragscode bevat de volgende elementen:

Medewerkers:
- Hoe om te gaan met geautomatiseerde informatiebeveiliging. Denk aan wachtwoordbeleid, opslaan van gegevens, document management.
- Hoe om te gaan met niet-geautomatiseerde informatiebeveiliging. Denk aan vergrendelen van werkplekken, afsluiten van deuren en kasten en hoe om te gaan met datadragers.
- Een fair use policy waarin OVO Zaanstad de kaders schetst voor privégebruik van bedrijfsmiddelen, en hoe dit privégebruik verantwoord plaats kan vinden. Denk hier aan gebruik van social media e.d.
- Gedragsregels over hoe om te gaan met data van OVO Zaanstad op privé-apparaten.
- De protocollen die gevolgd moeten worden wanneer er datalekken of andere inbreuken op de gegevensbescherming zijn.
- Hoe er omgegaan moet worden met gevallen waarin het bij een medewerker bekend is dat een andere medewerker bewust de gedragscode overtreedt (dit kan ook onderdeel uitmaken van de klokkenluidersregeling).

Deze gedragscode informatiebeveiliging kan deel uitmaken van een algemene gedragscode binnen OVO Zaanstad.

Leerlingen:
De gedragscode voor leerlingen dient, naast het duidelijk maken van de plichten van de leerling ten aanzien van datagebruik en -verwerking, ook een instructief doel. De code geeft de leerling handvatten om verantwoord datagebruik mogelijk te maken. OVO Zaanstad gaat actief voorlichting geven over deze gedragscode aan leerlingen.

- Hoe om te gaan met wachtwoorden verstrekt door OVO Zaanstad, denk aan wijzigen, hergebruik van wachtwoorden en het delen van wachtwoorden.

- Het beleid en de mogelijke gevolgen van het kopiëren en verder verspreiden van auteursrechtelijke beschermde gegevens die uitsluitend voor educatieve doeleinden aan de leerling ter beschikking zijn gesteld.
- Te volgen protocollen wanneer leerlingen een datalek vaststellen. Dit kan hun eigen gegevens betreffen, maar ook wanneer zij misbruik door medeleerlingen waarnemen.

5.10.2 Jaarverslag

Het College van Bestuur van OVO Zaanstad legt verantwoording af over het gevoerde informatiebeveiligingsbeleid. Om deze eindverantwoordelijkheid te kunnen dragen, moet het CvB periodiek geïnformeerd worden over de stand van zaken. Buiten dat er bij calamiteiten een crisisteam wordt samengesteld waar het CvB onderdeel van uitmaakt, brengen de privacy- en security-officer, samen met de informatiemanager, jaarlijks verslag uit aan bestuur en FG. Dit jaarverslag wordt per kalenderjaar opgesteld. Het CvB wordt over de volgende aspecten geïnformeerd:

- De uitkomsten van het jaarlijkse assessment, met aanbevelingen voor het volgend kalenderjaar;
- De voortgang op het verwerken van aanbevelingen uit het vorige assessment;
- Een overzicht van incidenten die in het afgelopen jaar zijn vastgelegd.

5.10.3 Assessment en audit

OVO Zaanstad kiest ervoor om met regelmaat een assessment uit te (laten) voeren om de kwaliteit van de informatiebeveiliging en het gevoerde beleid te toetsen. Het assessment wordt jaarlijks uitgevoerd door de afdeling Informatiemanagement van OVO Zaanstad. Elke drie jaar wordt een audit door een externe, onafhankelijke partij uitgevoerd.

5.10.4 Applicatieselectie

Conform de beleidsnotitie ICT en Onderwijs (september 2020) hanteert OVO Zaanstad de volgende uitgangspunten bij de aanschaf van onderwijsapplicaties:

a. Nieuw aan te schaffen applicaties zijn webbased en beschikbaar binnen een portaal;
b. De applicaties zijn AVG-proof;
c. Nieuw aan te schaffen devices zijn voorzien van Mobile Device Management.

OVO Zaanstad stelt de informatie- en gegevensbeveiliging centraal bij het maken van keuzes voor techniek. Dat betekent dat er enkel gebruik gemaakt wordt van informatiesystemen die ontwikkeld zijn volgens de principes van *privacy-by-design*. Dit houdt het volgende in:

- Informatiesystemen zijn met informatiebeveiliging als uitgangspunt ontwikkeld
- Opslag en verwerking van gegevens worden aan de hoogste standaarden getoetst
- We sluiten zoveel mogelijk aan bij DPIA's (zie voor een uitleg paragraaf 5.10.5) die op sectorniveau worden uitgevoerd (bijvoorbeeld door SIVON).

Daarnaast kiest OVO Zaanstad enkel voor nieuwe informatiesystemen als er recht gedaan kan worden aan de uitgangspunten van *privacy-by-default*. Dat houdt onder andere het volgende in:

- Er wordt zo min mogelijk informatie verzameld, alleen de hoogst noodzakelijke gegevens worden in het systeem vastgelegd.
- Gebruikers van wie gegevens worden vastgelegd hebben te allen tijde recht en mogelijkheid op inzage in de gegevens die over hun zijn vastgelegd.
- De bovenschools privacyofficer en Informatiemanager waken ervoor dat gegevens die voor een bepaald doel worden vastgelegd, niet voor een ander doel gebruikt worden.

5.10.5 Uitvoeren DPIA

Een Data Protection Impact Assessment (DPIA), ook wel gegevensbeschermings-effectbeoordeling (GEB) genoemd, is een instrument om privacy risico's van een gegevensverwerking in kaart te brengen, zodat een organisatie passende maatregelen kan nemen om de privacyrisico's te verkleinen. Een DPIA is een belangrijk instrument om te kunnen aantonen dat de organisatie voldoet aan de verplichtingen van de Algemene Verordening Gegevensbescherming (AVG).

Een DPIA wordt uitgevoerd om:

- te voldoen aan de wettelijke verplichting die voortvloeit uit artikel 35 van de AVG;
- privacyrisico's te analyseren, te identificeren en te minimaliseren;
- relevante stakeholders aanbevelingen te geven en/of te raadplegen over de AVG-compliance manier van werken;
- de verwerking van persoonsgegevens op te volgen en overzicht te behouden.

Voor OVO Zaanstad is dit een manier om privacy- en gegevensbeschermingsrisico's te identificeren en te minimaliseren. In een DPIA wordt de verwerking van persoonsgegevens beschreven, de noodzaak en evenredigheid ervan beoordeeld, de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen ingeschat en er worden maatregelen bepaald om deze risico's aan te pakken. Het is van belang om bij het uitvoeren van een DPIA de gevolgde methodiek en de uitkomsten vast te leggen.

OVO Zaanstad maakt zoveel mogelijk gebruik van DPIA's die op sectorniveau zijn uitgevoerd (bijvoorbeeld door SIVON) en maakt voortdurend een afweging tussen kosten en baten.

5.10.6 Registers

OVO Zaanstad beschikt over een dataregister, een register met incidentmeldingen en een register van verwerkersovereenkomsten. Al deze registers worden centraal beheerd door de functionaris gegevensbescherming.

5.10.7 Gebruik van analytics

OVO Zaanstad waakt ervoor dat geen van de scholen gebruik maakt van analysetools die leiden tot het opstellen van profielen van bezoekers van onze websites. Deze eis wordt opgenomen in de contracten met hostingproviders en leveranciers die betrokken zijn bij onze online dienstverlening.
Vindbaarheid in zoekmachines maakt geen onderdeel uit van deze policy, maar ook hier wordt terughoudendheid betracht. Het doel van OVO Zaanstad is om online goed vindbaar te zijn.

5.10.8 Geheimhoudingsplicht

Binnen OVO Zaanstad hebben medewerkers een geheimhoudingsplicht. Deze wordt genoemd in arbeidsvoorwaardengesprekken en is vastgelegd in de CAO (CAO VO 22-23 artikel 18.5). Voor medewerkers die geen dienstverband hebben, bijvoorbeeld externe inhuur, worden aparte verklaringen opgesteld.
Bij overtreding van regels kunnen disciplinaire maatregelen worden getroffen (CAO VO 22-23 artikel 10.8).

5.10.9 Cryptografische beheersmaatregelen

OVO Zaanstad neemt de volgende maatregelen m.b.t. het versleutelen van gegevens:

1. Alle inlogacties van medewerkers vinden plaats volgens multifactor autentificatie (toegang tot een systeem in twee stappen)
2. Bestandsoverdracht naar externen vindt alleen versleuteld plaats of via een teamssite
3. De inrichting van de ICT-omgeving vindt zo plaats dat versleuteling van gegevens de standaard is.

5.10.10 Classificatie

Het beveiligingsniveau van informatie wordt uitgedrukt in classificatieniveaus voor

- *Beschikbaarheid*: de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor de juiste gebruikers;
- *Integriteit*: de mate waarin gegevens of functionaliteit juist gedefinieerd en ingevuld zijn;
- *Vertrouwelijkheid*: de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Welk beveiligingsniveau geschikt is voor een bepaalde informatie, hangt af van de classificatie van de informatie die het systeem verwerkt. De bovenschoolse privacy-officer en de security-officer bepalen, in samenspraak met de functionaris gegevensbescherming, de classificatie. De vertrouwelijkheid van informatie is gebaseerd op privacywetgeving (AVG) en op eigen beleid.

Ten aanzien van de beschikbaarheidseisen worden de volgende klassen onderscheiden:

- Openbaar: de gegevens zijn algemeen toegankelijk
- Laag: algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de organisatie, haar medewerkers of de leerlingen en ouders;
- Midden: algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 24 uur brengt merkbare schade toe aan de belangen van de organisatie, haar medewerkers of de leerlingen en ouders;
- Hoog: algeheel verlies of niet beschikbaar zijn van deze informatie brengt direct merkbare schade toe aan de belangen van de organisatie, haar medewerkers of de leerlingen en ouders.

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 OVO Zaanstad.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	CvB 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)	Informatiemanager of Bovenschools privacy officer (de persoon die inhoudelijk verantwoordelijk is voor IBP)	• 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	Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming en/of Bovenschools Privacy officer	• Toezicht op naleving privacy wetgeving • Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.: ICT, HRM / P&O, facilitair, onderwijs, financiën, inkoop en administratie	• Classificatie / risicoanalyse in samenwerking met Manager IBP (Informatiemanager / verantwoordelijke IBP / privacy officer) • 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	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

		van gebruikers regelmatig beoordelen en controleren.	
Uitvoerend (operationeel)	Security officer Privacy-medewerkers op school Functioneel en/of applicatie beheerder Medewerkers Dagelijkse leiding / leidinggevende / directie	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten • Aanspreekpunt op school, uitdragen IBP-beleid, coachen en begeleide van collega's • Uitvoeren taken conform gegeven richtlijnen en procedures • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen, de situatie op 1 februari 2023. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Aanwezig?	Document	Bijzonderheden
	Verplicht vanuit AVG	
x	Procesbeschrijving melden datalekken	
x	Registratie beveiligingsincidenten	
	Dataregister om te voldoen aan de registratieplicht	
x	Verwerkersovereenkomsten	Privacy bijlage beschikbaar stellen
	Procedure gegevensbeschermingseffectbeoordeling	DPIA
	Risicoanalyse	
x	Functionaris voor Gegevensbescherming	Communicatie richting medewerkers
	Gewenst	
x	Procedure toestemming gebruik beeldmateriaal	Module in Magister
	Procedure voor verwijderen van gegevens	Bewaartermijnen
x	Communicatie rechten betrokkenen	Communicatie richting betrokkenen
x	Procesbeschrijving rechten betrokkenen	Proces rondom aanvragen van betrokkenen
	Privacyreglement	
	Autorisatiematrix	Wie mogen gegevens inzien, bewerken enz.
x	Afspraken gebruik sociale media	
	Procedure rondom training medewerkers	Bewustzijn creëren
x	Protocol gebruik camera- en videobeelden	
x	Wachtwoordbeleid	
	Responsible disclosure	
x	Gedragscode ict en internetgebruik	
	Acceptable use policy	Verantwoord gebruik bedrijfsmiddelen
	Procedure rondom uitwisselen gegevens	Passend onderwijs, leerling dossiers, leerplicht enz.