vereniging
ons middelbaar onderwijs
samen groeien

Informatiebeveiligings- en privacy beleid

Versie: 1.1 21 oktober 2025

Documentgeschiedenis

Revisies

Versie	Datum	Auteur	Review
0.1	21-2-2025	PO	Concept
0.2	25-2-2025	PO	Afstemming met en beoordeling door FG
0.3	6-3-2025	PO	Afstemming met concern controller
1.0	19-3-2025	PO	Beleidsdocument afgerond
1.1	14-4-2025	IB	Beleidsdocument uitgebreid met Informatiebeveiliging

Vaststelling

Naam	Functie	Versie	Datum
Raad van Bestuur		1.1	21 oktober 2025

Documentclassificatie

Classificatie	Beschrijving
Openbaar	Dit document mag zonder beperkingen worden gedeeld

Inhoudsopgave

1 Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. Lesmateriaal wordt digitaal aangeboden, toetsingsprogramma's worden digitaal en de resultaten en ontwikkelingen van leerlingen worden opgenomen in een digitaal leerlingvolgsysteem. Daarnaast wordt ook veel gebruikgemaakt van digitale communicatie tussen de school, leerlingen en ouders/verzorgers. Door deze ontwikkelingen neemt het risico op verstoring van het onderwijs, verlies of misbruik van gegevens en overmatige dataverzameling toe. Het is de verantwoordelijkheid van Ons Middelbaar Onderwijs (OMO) om dat te voorkomen en een veilige leeromgeving te bieden.

Dit beleid voor informatiebeveiliging en privacy (IBP-beleid) beschrijft hoe OMO omgaat met de beveiliging van informatie en hoe de verwerking van (persoons)gegevens wordt gewaarborgd en gehandhaafd. In het beleid worden de verschillende rollen en verantwoordelijkheden binnen OMO op het gebied van informatiebeveiliging en privacy (IBP) beschreven.

Het informatiebeveiliging- en privacybeleid is van toepassing op de gehele organisatie, namelijk de vereniging OMO en de scholen. Daarnaast is dit beleid ook van toepassing op het OMO-bureau.[1]

1.1 Onze intentie

OMO draagt de verantwoordelijkheid voor het creëren van een veilige werk- en leeromgeving. Dit houdt in dat OMO passende technische en organisatorische maatregelen toepast om informatie te beschermen en ongeoorloofde toegang, verlies of misbruik te voorkomen.
Het recht op privacy is een grondrecht. Iedereen heeft recht op privacy en bescherming van de persoonlijke levenssfeer. Dit geldt vanzelfsprekend ook voor leerlingen, ouders/verzorgers, medewerkers en docenten. OMO is verantwoordelijk voor het waarborgen van de privacy van de leerlingen en het personeel. Dit betekent ook dat deze betrokkenen zeggenschap hebben over het gebruik van hun persoonsgegevens, zoals wettelijk bepaald.
Bij OMO staat het bieden van goed onderwijs voorop. Om dit te kunnen doen verwerken wij diverse persoonsgegevens van leerlingen, ouders/verzorgers, medewerkers en docenten. OMO vindt het belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. Het goed regelen van informatiebeveiliging en privacy in een beleid is noodzakelijk om de gevolgen van mogelijke informatiebeveiliging- en privacyrisico's tot een aanvaardbaar niveau terug te brengen en de voortgang van het onderwijs te kunnen waarborgen.
Door het toenemende belang van digitalisering in het onderwijs zijn IT-risico's ook organisatierisico's geworden. Investeren in kwalitatieve goede en veilige ICT waarin continuïteit en beschikbaarheid gewaarborgd is, is daarom van belang.

1.2 Doelstelling

Dit beleid is erop gericht de kwaliteit van de verwerking van (persoons)gegevens en de beveiliging van informatie en systemen te verhogen. Hierbij moet een juiste balans bestaan tussen veiligheid, privacy, functionaliteit, gebruiksvriendelijk en inzet van capaciteit en middelen. Het uitgangspunt is dat iedere leerling en medewerker recht heeft op een veilige leer-/werkomgeving, daarbij de persoonlijke levenssfeer van de betrokkenen wordt gerespecteerd en OMO voldoet aan relevante wet- en regelgeving. Deze veilige leer-/werkomgeving heeft ook als doel de continuïteit van het onderwijs en de bedrijfsvoeringprocessen te waarborgen. Dit gebeurd door het voorkomen van beveiligingsincidenten en de eventuele gevolgen hiervan beperken.

[1] Artikel 26 Statuten vereniging OMO: Raad van Bestuur is bevoegd om het privacybeleid vast te stellen voor de gehele organisatie.

Dit gebeurt ook door onder andere door bewustwording te vergroten over het belang van het zorgvuldig omgaan met informatie, systemen en (persoons) gegevens.
OMO maakt gebruik van het 'Normenkader Informatiebeveiliging en Privacy voor het onderwijs' - oftewel het in de gehele onderwijssector gebruikte Normenkader IBP - om inzichtelijk te maken waar de organisatie nu staat en welke maatregelen genomen moeten worden om een veilige werkomgeving te creëren en te voldoen aan de AVG.

1.3 Reikwijdte

Dit beleid is van toepassing op alle leerlingen, docenten, medewerkers, bezoekers, ouders/verzorgers, derde partijen en andere gebruikers die toegang hebben tot of werken met de informatie van OMO. Het gaat bijvoorbeeld om leerlingdossiers, personeelsadministratie maar ook bestanden op ict-netwerken op de scholen. Het beleid heeft betrekking op de verwerking van alle soorten gegevens en informatie waaronder; persoonsgegevens, bedrijfsinformatie en technische gegevens.
Informatiebeveiliging en privacy maken integraal onderdeel uit van dit IBP-beleid. Informatiebeveiliging is een belangrijke voorwaarde voor privacy. Informatiebeveiliging omvat de beveiliging van alle informatie, terwijl privacy gaat over de verwerking van persoonsgegevens.

2 Juridisch kader

2.1 Wettelijke en reglementaire kaders

Het juridisch kader voor dit privacybeleid wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet UAVG. Daarnaast kunnen uit andere wet- en regelgeving verplichtingen of instructies voortvloeien voor de verwerking van (persoons)gegevens. Voor OMO is op dit gebied onder andere de volgende wetgeving van belang:

- Wet op het primair onderwijs
- Wet voortgezet onderwijs
- Wet op de expertisecentra
- Wet onderwijstoezicht
- Archiefwet en Archiefbesluit
- Leerplichtwet
- Wet medezeggenschap op scholen
- Arbeidsregelgeving en CAO
- Belastingwetgeving
- Telecommunicatiewet en e-privacy wetgeving
- EU AI Act
- Cyber Resilience Act
- Digital Services Act
- Cyberbeveiligingswet

Indien een (mogelijke) strijdigheid tussen dit beleid en de AVG en/of gerelateerde wet- en regelgeving bestaat, dan moet voorafgaand aan een verwerking overlegd worden met de privacy officer die zonodig de FG vraagt om advies.

2.2 Normen en standaarden

Het Normenkader Informatiebeveiliging en Privacy helpt scholen om de digitale veiligheid te verhogen. Met dit normenkader spreekt de onderwijssector af wat de minimale eisen zijn voor digitaal veilig onderwijs, zodat elke school

hieraan kan voldoen. Het doel is dat alle leerlingen, ouders en medewerkers erop kunnen rekenen dat zij leren en werken in een digitaal veilige schoolomgeving en dat hun (persoons)gegevens worden beschermd.

Het Normenkader IBP bestaat uit 69 normen voor informatiebeveiliging en 25 normen voor privacy. Het Normenkader IBP is ontwikkeld in samenwerking met het onderwijs op initiatief van het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad. Het deel Informatiebeveiliging is gebaseerd op het model van de Nederlandse Beroepsvereniging van Accountants (NBA). Dit model wordt ook door SURF gehanteerd. Het deel Privacy komt voort uit het SURF audit Toetsingskader Privacy, dat is afgeleid van het "Borgingsproduct AVG" van de IBD/VNG. Door de samenwerking op te zoeken met zowel SURF als MBO Digitaal wordt in de gehele onderwijssector toegewerkt naar dezelfde standaard voor informatiebeveiliging en privacy.

OMO kiest ervoor om ook toe te werken naar dat ene normenkader om aan de minimale vereisten te voldoen voor digitaal veilig onderwijs. Dit is het 'Normenkader Informatiebeveiliging en Privacy voor het onderwijs'. Dit normenkader bevat voor OMO de regels, principes en standaarden op het gebied van informatiebeveiliging en privacy waaraan OMO moet voldoen voor een digitale veilige schoolomgeving.

3 Eigenaarschap en verantwoordelijkheden

Dit hoofdstuk beschrijft hoe de verschillende rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy samenhangen.

3.1 Rollen en verantwoordelijkheden met betrekking tot verwerking van (persoons)gegevens

Om de verwerkingen van gegevens gestructureerd en gecoördineerd op te pakken, wordt bij OMO een aantal rollen onderkend die aan functionarissen in de bestaande organisatie zijn toegewezen. Informatiebeveiliging en privacy bij OMO is ingericht volgens het Three Lines model (3L-model). Het 3L-model is een leidraad bij het inrichten van de governance van een organisatie. In paragraaf 3.2 wordt verder ingegaan op dit model. Hieronder worden de verschillende rollen benoemd dit in dit model opgenomen zijn.

Raad van Bestuur
De Raad van Bestuur is de verwerkingsverantwoordelijke en daarmee de eindverantwoordelijke voor de rechtmatige en zorgvuldige verwerking van gegevens binnen OMO en stelt het beleid, de maatregelen en de procedures op het gebied van informatiebeveiliging- en privacy vast. Binnen het bestuur hebben één of meerdere bestuurders IBP in hun aandachtsgebied.

Schooldirecteuren en rectoren
De directies/rectoraten van de, bij OMO aangesloten, scholen zijn verantwoordelijk voor de uitvoering van dit beleid op hun eigen school en rapporteren, wanneer nodig, aan de Raad van Bestuur over de stand van zaken op het gebied van het verwerken van persoonsgegevens binnen de eigen school. De rector/directeur draagt zorg voor het adequaat beveiligen van persoonsgegevens van het personeel en de leerlingen van de school.[2]

Leidinggevende
Het creëren van bewustwording en de naleving van het beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:
- ervoor te zorgen dat zijn/haar medewerkers op de hoogte zijn van het beleid;
- toe te zien op de naleving van het beleid door zijn/haar medewerkers;
- periodiek het onderwerp informatiebeveiliging en privacy onder de aandacht te brengen in werkoverleggen.

[2] Artikel 22 Huishoudelijk reglement

Privacy Officer

De Privacy Officer is verantwoordelijk voor het ontwikkelen en uitvoeren van dit beleid, zorgt ervoor dat privacy taken worden uitgevoerd en dat privacy maatregelen ingebed worden in de organisatie, zowel voor de scholen als voor het OMO-bureau.

- Inhoudelijk verantwoordelijk voor uitwerking van het privacybeleid;
- Adviseert verwerkingsverantwoordelijke, scholen over privacybeleid;
- Uitwerken algemeen privacybeleid naar specifiek beleid op een uniforme manier;
- Opstellen en beheren van processen, richtlijnen en procedures om de uitvoering van het privacybeleid te ondersteunen;
- Awareness over privacy binnen de organisatie;
- Aanspreekpunt voor privacy-contactpersonen;
- Bewaakt de kwaliteit van het register van verwerkingen;
- Ondersteunt bij Data Protection Impact Assessments (DPIA's) en bij pré DPIA's;
- Adviseert in geval van (het vermoeden van) datalekken en -incidenten.

Privacy-contactpersoon

OMO heeft voor elke school een privacy-contactpersoon benoemd en hen daarvoor uren beschikbaar gesteld om hun werkzaamheden uit te kunnen voeren. Een privacy-contactpersoon is iemand die verantwoordelijk is voor het veilig en verantwoord gebruik van persoonsgegevens van leerlingen, medewerkers en andere betrokkenen, binnen de school van de leerlingen, medewerkers en andere betrokkenen (ouders/verzorgers, bezoekers, leveranciers) op hun school/college. Hij/zij zal nauw samenwerken met systeemeigenaren (systeemeigenaar is iemand die verantwoordelijk is voor een belangrijk systeem, platform of applicatie, waarmee een of meerdere processen worden ondersteund) en de ICT contactpersoon op hun school.

De privacy-contactpersonen bij de scholen worden actief en direct ondersteund door de OMO brede Privacy Officer en de Security officer.

De privacy-contactpersoon heeft onder meer de volgende taken:

- Interne vraagbaak voor privacyvragen
- Het (laten) opnemen van specifieke verwerkingen op hun school, van persoonsgegevens in het register.
- Het (laten) maken van schriftelijke afspraken over het delen van persoonsgegevens zoals een verwerkersovereenkomst.
- Het ondersteunen bij het in beeld brengen van risico's (o.a. bij een Data Protection Impact Assessment of DPIA).
- Het (laten) uitvoeren van de maatregelen die nodig zijn om de risico's te beperken.
- Het functioneren als eerste aanspreekpunt voor de eigen school op het gebied van privacy.
- Het tijdig signaleren van privacy risico's.
- Het op de eigen school begeleiden van en juiste wijze uit laten voeren van de rechten van betrokkenen, zoals inzageverzoeken, en dit inzageverzoek afstemmen met de privacy officer.
- Het functioneren als contactpersoon voor de Functionaris Gegevensbescherming OMO en/of Privacy Officer OMO.

Functionaris voor Gegevensbescherming

OMO heeft een interne toezichthouder op de verwerking van persoonsgegevens aangesteld. Deze toezichthouder wordt Functionaris voor Gegevensbescherming genoemd (hierna: "FG"). De FG heeft wettelijk verankerde taken en is onafhankelijk. Dat betekent dat de FG geen instructies mag krijgen van het bestuur bij het uitvoeren van de toezichthoudende taken.

De FG wordt door OMO tijdig betrokken bij alle aangelegenheden waar persoonsgegevens worden verwerkt. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie bij OMO. OMO meldt de FG aan bij de toezichthoudende autoriteit (AP).

De taken van de FG zijn:

- Gevraagd en ongevraagd advies geven over de omgang met persoonsgegevens en de bescherming van privacy van leerlingen, medewerkers en andere betrokkenen.

- Het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG.
- Het toezien op de naleving van de AVG en andere relevante privacywetgeving.
- Het toezien op de naleving van dit beleid.
- Toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van he betrokken personeel en de betreffende audits, adviseren over en toezien op de uitvoering van DPIA's.
- Het behandelen van klachten en/of vragen die rechtstreeks aan de FG zijn gericht.
- Het samenwerken met de toezichthoudende autoriteit.
- Fungeren als eerste aanspreekpunt voor de toezichthoudende autoriteit.

CISO

De CISO heeft een strategische en beleidsmatige rol in de informatiebeveiligingsorganisatie. Deze functionaris houdt zich op strategisch/visie vlak bezig met informatiebeveiliging binnen de hele vereniging. Weet kaders en richtlijnen op te stellen en kan snel schakelen in geval van grootschalige incidenten. Het is de rol van de CISO om te rapporteren richting de RvB over de PDCA-cyclus en naleving van het centraal opgestelde Informatiebeveiligingsbeleid. Dit zal op basis van de input vanuit de security officer gebaseerd zijn. De CISO controleert de ICT-afdelingen op securityrisico's.

Security Officer

De security officer heeft een tactische en operationele rol in de informatiebeveiligingsorganisatie. De security officer implementeert het informatiebeveiligingsbeleid. Het is de rol van de security officer om de opvolging van deze acties te monitoren als onderdeel van de PDCA-cyclus en hierover te rapporteren richting bestuur via de CISO.
Tot slot is de security officer het eerste aanspreekpunt voor de volledige vereniging voor informatiebeveiliging gerelateerde onderwerpen.

ICT-contactpersoon

De ICT-contactpersoon heeft voornamelijk een rol in de IB-organisatie bij incidenten en in kleinere mate bij de verantwoording. Bij een grootschalig incident dient de ICT-contactpersoon snel te kunnen schakelen met de functionaris IB en andere van belang zijnde actoren om mogelijke gevolgschade te beperken. Veel incidenten op het gebied van informatiebeveiliging en privacy hebben een IT-component in zich (denk aan ransomware, DDoS aanval, phishing). Het is daarom van belang dat hier een inhoudsdeskundige is aangesloten. Binnen de verantwoordingsstructuur is de ICT-contactpersoon ook van belang voor het opstellen van de rapportages, daar er veel informatie nodig is vanuit deze rol. De ICT-contactpersoon heeft echter geen actieve rol bij het opstellen van de rapportage zelf, maar voorziet de IB-coördinator en IB-rapporteur wel van input.

Functionaris Informatie Beveiliging

De functionaris IB heeft een rol in de IB-organisatie bij incidenten en bij verantwoording. Deze functionaris houdt zich op strategisch/tactisch vlak bezig met informatiebeveiliging. Weet kaders en richtlijnen op te stellen en kan snel schakelen in geval van grootschalige incidenten. Daarnaast dient deze functionaris de rapportages binnen de verantwoordingsstructuur goed tot zich te nemen en de eventuele tekortkomingen samen met de verantwoordelijke medewerkers te vertalen in acties. Het is de rol van de functionaris IB om de opvolging van deze acties te monitoren als onderdeel van de PDCA-cyclus.
Tot slot is de functionaris IB het eerste aanspreekpunt binnen de school voor informatiebeveiliging gerelateerde onderwerpen.

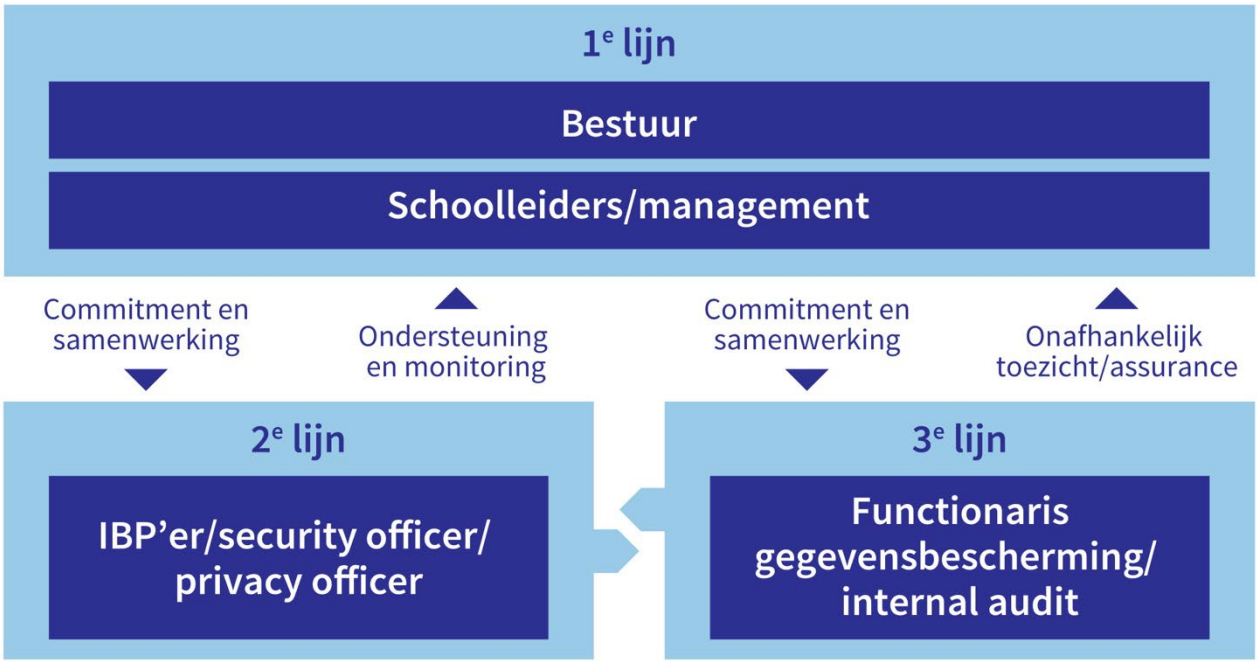
Awareness Coördinator

De Awareness Coördinator is verantwoordelijk voor bewustwording van IB en privacy binnen de school. In de praktijk houdt dit in dat deze functionaris initieert, coördineert en uitvoert binnen de organisatie op het gebied van bewustwording. Hierbij kan gedacht worden aan nieuwsbrieven, aanbieden van posters, activiteiten, quizzen en dergelijken.

3.2 Three Lines model

Hierbij werkt OMO toe naar het 3-lines of defense model. Dit model helpt OMO risico's te beheersen door verantwoordelijkheden te verdelen over drie verdedigingslinies. De eerste lijn bestaat uit medewerkers in het primaire onderwijsprocessen: de scholen beheren de risico's binnen dagelijkse processen. De tweede lijn biedt ondersteuning, monitoring en expertise, het gaat hier om de privacy officer (PO) en security officer. In de derde lijn zijn de Functionaris voor Gegevensbescherming (FG) en Chief Information Security Officer (CISO) werkzaam die onafhankelijke beoordeling, ondersteuning en advisering leveren en zich richten op risicobewaking & compliance en werkt toe naar onafhankelijke interne auditing. Deze drie lijnen opereren onder verantwoordelijkheid van het bestuur.

Informatiebeveiliging en privacy bij OMO is ingericht volgens het Three Lines model (3L-model). Het 3L-model is een leidraad bij het inrichten van de governance van een organisatie.



3.2.1 Eerste lijn: eindverantwoordelijkheid bij het bestuur

Het 3L-model heeft als uitgangspunt dat de eerste lijn verantwoordelijk is voor processen, informatie en systemen van de organisatie, de risico's die hieruit voortvloeien en het treffen van de juiste maatregelen om de risico's te verkleinen. De eerste lijn bestaat uit het bestuur, rectoren, directeuren en schoolleiders, en het verdere lijnmanagement van OMO.
Het bestuur is binnen de eerste lijn eindverantwoordelijk voor privacy, maar kan bepaalde verantwoordelijkheden beleggen bij andere functies binnen de organisatie. Bij de beschrijving van de beleidsthema's in hoofdstuk 4 en 6 wordt per thema beschreven wie er verantwoordelijk is.

Op de scholen houden de privacy contactpersonen zich bezig met privacy op de eigen school en de ict-contactpersonen met ict op de eigen school. Zij overleggen zo nodig met deskundigen uit de tweede lijn.

3.2.2 Tweede lijn: adviseren en ondersteunen

Naast de eerste lijn moet er een rol zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management de verantwoordelijkheden ook daadwerkelijk neemt. De tweede lijn bestaat uit security officers, privacy officers, IBP-adviseurs en juridische adviseurs bij het OMO Bureau.

3.2.3 Derde lijn: onafhankelijke controle

De derde lijn controleert of de eerste en tweede lijn soepel samenwerken en goed functioneren. De derde lijn is onafhankelijk, opereert los van de andere organisatieonderdelen en suggereert waar nodig verbeteringen. De functionaris voor gegevensbescherming (FG), CISO en concern controller vallen binnen de derde lijn. De FG wordt aangesteld door het bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een reglement dat door het bestuur wordt vastgesteld.

3.3 Medezeggenschap

OMO betrekt de medezeggenschapsraad bij besluiten over regelingen en procedures ten aanzien van de bescherming van persoonsgegevens. OMO is eindverantwoordelijk voor het informeren van de medezeggenschapsraad en voor het opstellen van instemmingsprocedures.

Voor het beleid dat OMO-breed (voor de vereniging, de scholen en het OMO-bureau) van toepassing is, wordt de GMR geraadpleegd. Voor beleid dat op het niveau van een specifieke school wordt vastgesteld, wordt de MR van de school geraadpleegd. Het schoolbestuur is verantwoordelijk voor het informeren van de medezeggenschapsraad en voor het opstellen van instemmingsprocedures.

4 Uitgangspunten informatiebeveiliging

Om richting te geven aan de uitvoering van informatiebeveiliging en ter ondersteuning van besluitvorming hierover zijn beveiligingsprincipes opgesteld. Beveiligingsprincipes verwoorden wat deze organisatie belangrijk vindt en zijn de beweegredenen voor gedrag in de organisatie. Binnen Ons Middelbaar Onderwijs worden de volgende beveiligingsprincipes gehanteerd:

1. **Raad van bestuur neemt verantwoordelijkheid**

De Raad van Bestuur (RvB) van OMO neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy op orde is. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke. Op schoolniveau is de rector/algemeen directeur verantwoordelijk voor een veilige digitale omgeving;

2. **Informatiebeveiliging binnen OMO is ieders verantwoordelijkheid.**

Er wordt ingezet op een lerende cultuur waarin informatiebeveiliging bevorderd wordt. Van medewerkers en externe partners wordt verwacht dat ze actief bijdragen aan de veiligheid van informatie en informatiesystemen, dat zij alert zijn op risico's van hun eigen handelen en bij twijfel zullen zij de daarvoor aangewezen experts raadplegen;

3. **Gezamenlijk organiseren**

Binnen OMO zetten we in op het gezamenlijke organiseren van de ICT en Informatiebeveiliging. Gezamenlijk zijn we beter instaat om bestand te zijn tegen toenemende dreigingen en kan er beter verantwoordelijkheid genomen worden op gebied van informatiebeveiliging;

4. **IBP-normenkader Funderend Onderwijs**

Binnen OMO wordt het IBP-normenkader Funderend Onderwijs (Versie juni 2024) als uitgangspunt genomen. Dit normenkader kent verschillende volwassenheidsniveaus. OMO (de scholen en het OMO-Bureau) streeft bij alle normen in het normenkader naar minimaal volwassenheidsniveau 3 vanaf 1 januari 2027;

5. **PDCA cyclus**

Informatiebeveiliging is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten de organisatie maken het noodzakelijk om periodiek te controleren of er nog wel de juiste beveiligingsmaatregelen worden gehanteerd. Dit gebeurt door het uitvoeren van (interne en externe) audits;

6. **Samenhangend stelsel van maatregelen**

Informatiebeveiliging binnen OMO omvat een samenhangend stelsel van maatregelen omtrent de aspecten techniek, mens en organisatie. Dit betekent dat de verschillende maatregelen die samen de informatiebeveiliging vormen niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan;

7. **Technische maatregelen**

Binnen OMO zijn passende technische (beveiligings-)maatregelen genomen om gegevens (incl. persoonsgegevens) te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren;

8. **Security by design en security by default**

Bij alle (ICT-) wijzigingen en vernieuwingen, zoals bijvoorbeeld het ontwerp en de aanschaf en/of ontwikkeling van nieuwe (informatie)systemen, wordt vanaf de start rekening gehouden met informatiebeveiliging en privacy zodat tijdig de juiste maatregelen genomen kunnen worden (security by design);

9. **Digitaal tenzij**

Alle informatie binnen de organisatie is (zoveel mogelijk) digitaal beschikbaar. Dit geldt zowel voor inhoudelijke informatie als procesinformatie;

10. **Risk based aanpak**

De aanpak van informatiebeveiliging van Ons Middelbaar Onderwijs is 'risk based'. Deze aanpak maakt het mogelijk om op basis van een voorafgaande risicoanalyse en (zelf)evaluatie prioriteiten te stellen en maatregelen te definiëren. De risicoanalyse is een fundamenteel onderdeel van de IB-aanpak bij OMO en de zelfevaluatie is gebaseerd op het IB-normenkader Funderend Onderwijs;

11. **Service Level Agreements**

Met leveranciers en netwerkpartners zijn afspraken gemaakt over de manier waarop wordt omgegaan met de uitwisseling van gegevens. Waar nodig in de vorm van een (verwerkers)overeenkomst. Bij het delen van informatie met leveranciers en netwerkpartners staat de veiligheid van gegevensuitwisseling voorop. OMO doet uitsluitend een beroep op (ICT-)-leveranciers die afdoende garanties kunnen bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen en dat zij proactief zijn in het aanpassen van hun systemen aan veranderende wet- en regelgeving en hierover actief communiceren. De continuïteit van alle belangrijke applicaties en functionaliteiten is gewaarborgd door middel van Service Level Agreements (SLA's);

12. **Preventie**

Binnen OMO zijn middelen (systemen, plannen en procedures) ingericht om potentiële dreigingen tijdig te kunnen signaleren en maatregelen om de effecten van incidenten zoveel mogelijk te reduceren en het herstel te bespoedigen;

13. **Mensen en middelen**

De organisatie stelt de benodigde mensen en middelen beschikbaar om de informatie te kunnen beveiligen volgens de wijze gesteld in dit beleid;

14. Samenwerken binnen informatiebeveiliging

Binnen OMO is samenwerken op gebied van Informatiebeveiliging de norm. Dit betekent dat samenwerking tussen de OMO-scholen zoveel mogelijk gestimuleerd wordt. Ook wordt de samenwerking opgezocht met andere onderwijsorganisaties, sectororganisaties binnen het funderend onderwijs en andere relevante derden. Als grootste onderwijsinstelling voor Voortgezet onderwijs zijn we toonaangevend op dit onderwerp;

5 Beleidsthema's informatiebeveiliging

5.1 Risicomanagement

OMO hanteert een losstaand risicomanagementbeleid. Dit is op dit moment in ontwikkeling en zal naar verwachting in het derde kwartaal 2025 bij de raad van bestuur voorgelegd worden.

5.2 Kennis en afhankelijkheid medewerkers

OMO is voor de beveiliging van informatie en de continuïteit van het onderwijs afhankelijk van de kennis en beschikbaarheid van medewerkers. OMO wil voorkomen dat er onvoldoende kennis aanwezig is bij medewerkers of dat kritieke kennis en vaardigheden onvoldoende aanwezig zijn binnen de organisatie. Taken van sleutelfiguren moeten daarom altijd overgenomen kunnen worden door andere medewerkers. Hiervoor hanteert OMO de volgende maatregelen:

- Een back-upplan voor kritieke medewerkers.
- Voldoende training en certificering.
- Een indienst-/uitdiensttredingproces waarin rekening gehouden wordt met aansluiting op het proces voor het beheren van rechten en rollen, de overdracht van kennis en documentatie en screening van medewerkers.

Verantwoordelijkheden :

- De raad van bestuur is verantwoordelijk voor het formeel goedkeuren van het back-upplan voor kritieke medewerkers.
- De manager HR is verantwoordelijk voor het opstellen en het beheren van het back-upplan voor kritieke medewerkers.
- De teamleider personeel- en salarisadministratie is verantwoordelijk voor het opstellen en het beheren van het indienst/ uitdiensttreding proces.

5.3 Bedrijfscontinuïteit

OMO zorgt ervoor dat mogelijke verstoringen van het onderwijs zo snel mogelijk verholpen worden en dat de impact van verstoringen beperkt blijft. Door processen te analyseren worden de meest kritieke applicaties en medewerkers geïdentificeerd, en wordt bepaald welke terugvalopties nu aanwezig zijn. Hierna kunnen maatregelen geïmplementeerd worden om verstoringen zo veel mogelijk te voorkomen of de impact te beperken. Er is een crisismanagementteam aanwezig om snel en adequaat op incidenten te reageren.

OMO hanteert de volgende maatregelen voor bedrijfscontinuïteit:

- Business impact analyses (BIA) op basis van de processen van de organisatie. De processen worden op basis van een risicogestuurde aanpak geanalyseerd, waarbij eerst de meest kritieke processen behandeld worden.

Nieuwe risico's die tijdens deze BIA's geïdentificeerd zijn, worden opgenomen in het risicoregister. Zie hiervoor het risicomanagementbeleid.
- Een bedrijfscontinuïteitsplan (BCP). Een crisismanagementaanpak waaronder periodieke crisisoefeningen maken onderdeel uit van het BCP. Taken en verantwoordelijkheden zijn duidelijk toegewezen in het BCP. Het BCP wordt na een jaarlijkse oefening steeds geactualiseerd.

Verantwoordelijkheden:
- Het bestuur is verantwoordelijk voor het formeel goedkeuren van het bedrijfscontinuïteitsplan.
- De concern controller is verantwoordelijk voor het opstellen en het beheren van het bedrijfscontinuïteitsplan.
- De CISO is verantwoordelijk voor het opstellen en het beheren van het ICT- bedrijfscontinuïteitsplan.

5.4 Back-up en herstel

Om de impact van verstoringen of dataverlies te beperken zorgt OMO voor back-ups van systemen en data. Op basis van de BIV-classificatie van systemen worden de back-upvereisten voor de systemen en de data binnen deze systemen vastgesteld. Back-ups worden regelmatig getest om te verifiëren of gegevens kunnen worden hersteld binnen de vastgestelde periode.

De volgende uitgangspunten worden hierbij gehanteerd:
- De proceseigenaar is degene die beslist over de continuïteitsvereisten van een dataverwerking of een systeem. Het initiatief voor deze afweging komt van de systeemeigenaar.
- We stellen dezelfde back-upeisen aan diensten van externe leveranciers als aan systemen die we zelf beheren.
- Bij voorkeur maken we bij externe leveranciers gebruik van de back-upfaciliteit die ze zelf bij hun dienst aanbieden. Ontbreekt die of voldoet die niet, dan maken we zelf back-ups van de informatie die we verwerken in de dienst van deze leverancier.
- We evalueren jaarlijks de manier waarop we zelf back-ups maken.

Verantwoordelijkheden:
- OMO stelt een procesbeschrijving op voor back-up en herstel.
- De Raad van Bestuur is verantwoordelijk voor het formeel goedkeuren van de back-up en herstel procesbeschrijving.
- De teamleider ICT is verantwoordelijk voor het opstellen en het beheren van de back-up en herstel procesbeschrijving.
- De systeemeigenaar is verantwoordelijk voor het toepassen van het back-up en herstel proces.

5.5 Fysieke beveiliging

OMO hanteert een losstaand Fysiek beveiligingsbeleid. Zie het document 20250114 OMO PH.01 Fysieke beveiligingsmaatregelen (0.1) en het document 20250114 OMO PH.02 Beheer van fysieke toegangsrechten (0.1).

5.6 Systeem- en data-eigenaarschap en configuratiebeheer

Om IT-processen te beheren is inzicht nodig in welke systemen worden gebruikt binnen de organisatie. Veel van de IBP-thema's in dit beleid zijn afhankelijk van dit inzicht. De rol van systeemeigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die specifiek voor een systeem gelden. De rol van data- eigenaar en die van data-steward wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die te maken hebben met een specifiek proces.

Voor het vastleggen van processen en het eigenaarschap van systemen en processen treftOMO de volgende maatregelen:

- OMO heeft een configuratiemanagementdatabase (CMDB) waarin alle systemen, het eigenaarschap en andere benodigde eigenschappen bijgehouden worden.
- Systeemeigenaarschap wordt bepaald vóór implementatie van nieuwe systemen. De eigenaren van systemen worden vastgelegd in het CMDB.
- Proceseigenaarschap wordt bepaald en vastgelegd binnen het verwerkingsregister.

Verantwoordelijkheden:

- De configuratiemanager is verantwoordelijk voor het opstellen en het beheren van de CMDB.
- De systeemeigenaar van elk systeem is verantwoordelijk voor het vastleggen van de juiste eigenschappen in de CMDB.

5.7 Classificatie van systemen en data

Om risicogestuurd beslissingen te kunnen nemen is belangrijk om per systeem het benodigde niveau van beschikbaarheid, integriteit en vertrouwelijkheid (BIV) te bepalen. De classificatie is beperkt tot systeemniveau. OMO kiest ervoor om de classificatie niet per individueel dataobject toe te passen. OMO heeft voor elk systeem dat opgenomen is in de CMDB een BIV-classificatie uitgevoerd. Deze BIV-classificatie wordt gebruikt om te bepalen welke maatregelen er voor het betreffende systeem geïmplementeerd moeten worden.

Voor het goed toepassen van de BIV-classificatie treft OMO de volgende maatregelen:

- De BIV-classificatie wordt uitgevoerd vóór de aanschaf van een nieuw systeem. Zie beleidsthema 4.11.
- De BIV-classificatie wordt vastgelegd in de CMDB.

Verantwoordelijkheden:

- De systeemeigenaar van elk systeem is verantwoordelijk voor het uitvoeren van de BIV-classificatie en het vastleggen hiervan in de CMDB.

5.8 Securitybaseline

Een securitybaseline voor IT-systemen is vastgesteld om het risico van ongeoorloofde toegang tot IT-middelen te beperken. OMO maakt gebruik van het certificeringsschema ROSA als securitybaseline voor IT-systemen in eigen beheer. De securitybaseline is formeel vastgelegd, wordt periodiek geactualiseerd en wordt goedgekeurd door het schoolbestuur. De toepassing van de securitybaseline voor IT-middelen wordt periodiek beoordeeld op naleving. Afwijkingen van de baselines zijn gedocumenteerd en goedgekeurd.

Verantwoordelijkheden:

- De Raad van Bestuur is verantwoordelijk voor het formeel goedkeuren van de securitybaseline.
- De systeemeigenaar van elk systeem is verantwoordelijk voor het voldoen aan de securitybaseline en het vastleggen van afwijkingen op de baseline.

5.9 Bewustwording

Beleid en technische maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hierin ook een belangrijke factor. Daarom wordt het bewustzijn van medewerkers over de

verantwoordelijkheden die ze hebben voortdurend aangescherpt, zodat de kennis van bestaande risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

Hiervoor neemt OMO de volgende maatregelen:

- Er is een bewustwordingsprogramma dat jaarlijks herzien wordt waarin de bewustwordingsactiviteiten en de verantwoordelijkheden voor deze activiteiten beschreven worden.

Verantwoordelijkheden:

- De Raad van Bestuur is verantwoordelijk voor het formeel goedkeuren van het bewustwordingsprogramma.
- De Privacy officer en security officer zijn verantwoordelijk voor het opstellen en het beheren van het bewustwordingsprogramma.

5.10 Incident- en problemmanagement

Incidentmanagement is het proces voor het melden van incidenten binnen de organisatie. Sommige incidenten kunnen een datalek tot gevolg hebben. Incidenten binnen de organisatie zijn nooit helemaal uit te sluiten. Een helder beschreven incidentmanagementproces is aanwezig om incidenten op tijd te herkennen en ze adequaat af te handelen.
De manier waarop dat gebeurt is vastgelegd in een procesbeschrijving waarbij de volgende onderwerpen minimaal terugkomen:

- Een centraal punt voor het melden van incidenten.
- Incidentenregister: Binnen dit incidentenregister wordt er duidelijk onderscheid gemaakt tussen datalekken en andere type incidenten.
- De classificatie van incidenten: Bij elk incident moet worden vastgesteld om wat voor type incident het gaat (beveiliging, privacy, etc.)
- De afhandeling van het incident: Het is duidelijk wie bij welk type incident betrokken moeten worden en wie verantwoordelijk is voor het afhandelen van de incidenten.
- Problemmanagement: Indien incidenten regelmatig terugkomen worden deze aangemerkt als een known error. De procesbeschrijving beschrijft de vervolgstappen voor een terugkerend incident.
- Monitoren en rapporteren: Afhandeling van incidenten en problemen worden gemonitord. Hierover wordt periodiek gerapporteerd.

Verantwoordelijkheden:

- De Raad van Bestuur is verantwoordelijk voor het formeel goedkeuren van de incidentmanagemenprocesbeschrijving.
- De teamleider ICT is verantwoordelijk voor het opstellen en het beheren van de incidentmanagementprocesbeschrijving.
- De incidentmanager is verantwoordelijk voor het inrichten en beheren van het incidentenregister.

5.11 Risicomanagement leveranciers

OMO besteedt een deel van de IT uit aan leveranciers, maar blijft eindverantwoordelijk voor beveiliging van informatie en persoonsgegevens.

Om ervoor te zorgen dat ook leveranciers zich houden aan de technische maatregelen die volgen uit de securitybaseline zijn bepaalde stappen toegevoegd aan het leveranciersmanagementproces:

- Er is een lijst met maatregelen opgesteld op basis van de securitybaseline van OMO.
- Er is een leveranciersmanagementproces waar de volgende stappen onderdeel van zijn:
- Voor de aanschaf van een nieuw systeem wordt een BIV-classificatie uitgevoerd.

- Op basis van deze BIV-classificatie en de lijst met maatregelen worden aanbestedingseisen opgesteld.
- Er wordt een periodieke controle gedaan op het voldoen aan de aanbestedingseisen.

Verantwoordelijkheden:

- De Raad van Bestuur is verantwoordelijk voor het formeel goedkeuren van de leveranciersmanagementprocesbeschrijving.
- De teamleider ICT is verantwoordelijk voor het opstellen en het beheren van de leveranciersmanagementprocesbeschrijving.
- De systeemeigenaar is verantwoordelijk voor de periodieke controle op het voldoen aan de aanbestedingseisen.

5.12 Werkplekken en mobiele apparaten

Persoonsgegevens en andere informatie uit systemen die binnen onze organisatie worden gebruikt, worden ontsloten via verschillende apparaten zoals laptops, tablets, smartphones en desktop-pc's. Deze apparaten brengen risico's met zich mee op het gebied van beveiliging, dataverlies en compliance.

Daarom treft OMO de volgende maatregelen:

- OMO hanteert een richtlijn voor het gebruik van werkplekken en mobiele apparaten.

Verantwoordelijkheden:

- De teamleider ICT is verantwoordelijk voor het formeel goedkeuren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten.
- De kwartiermaker ICT advies is verantwoordelijk voor het opstellen en het beheren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten.

5.13 Identiteits- en toegangsbeheer

OMO heeft een apart IAM-beleid waar op dit moment de laatste hand aan gelegd wordt.

5.14 Vulnerabilitymanagement en pentesting

Vulnerabilitymanagement en pentesting vormen een essentieel onderdeel voor het verminderen van risico's, het voorkomen van ongeautoriseerde toegang tot IT-systemen en het beschermen van gegevens tegen mogelijke dreigingen.

5.14.1 Threat intelligence & kwetsbaarheidsidentificatie

- Dreigingsinformatie wordt (threat intelligence) verzamelt uit onder andere CVE-databases, vendor bulletins, bug bounty-meldingen en berichten van school-CERT.
- Voortdurend worden er (geautomatiseerd) vulnerability scans uitgevoerd én zetten we periodiek penetratietests in om zowel intern als extern inzicht te krijgen in bestaande of nieuwe kwetsbaarheden.
- Vanuit leveranciers en de bredere securitycommunity ontvangt OMO advisories en waarschuwingen, die actief worden opvolgt om eventuele risico's voor onze IT-omgeving snel te herkennen en te adresseren.

5.14.2 Triage & risicoanalyse

- Zodra er kwetsbaarheden worden gesignaleerd, wordt de relevantie en impact hiervan op onze systemen en data bepaald.
- Prioritering vindt plaats volgens een vast scoringsmechanisme (bijvoorbeeld op basis van CVSS) om te bepalen welke kwetsbaarheden als eerste moeten worden aangepakt.
- Uitkomsten van vulnerability scans en penetratietests worden gecombineerd met andere threat intelligence-informatie voor een volledig risicobeeld, zodat er gerichte maatregelen genomen kunnen worden.

5.14.3 Melden & samenwerken met School-CERT en SOC

- Bij het ontdekken van kritieke kwetsbaarheden of dreigingen met hoog risico wordt direct het interne SOC (Security Operations Center) ingeschakeld voor verdere analyse en continue monitoring.
- School-CERT ontvangt een melding met de ernst en mogelijke indicators of compromise (IoC's). Zij leveren extra threat intelligence en adviseren over vervolgstappen.
- In overleg met School-CERT bepaalt het SOC of verdere escalatie, zoals extra monitoring of een verhoogd alert-niveau, noodzakelijk is.

5.14.4 Maatregelen & mitigatie

Op basis van de bevindingen plannen worden mitigatieacties geëvalueerd:

- Patches en updates worden uitgevoerd volgens het beleid in Patchmanagement.
- Configuratieaanpassingen vinden plaats conform het afgesproken configuratiemanagementproces, bijvoorbeeld bij het wijzigen van netwerk- of serverinstellingen.
- Compensating controls, zoals tijdelijke firewall-regels of netwerkgroepsegmentatie, zetten wij in wanneer directe patching niet haalbaar is of aanvullende bescherming vereist is.

5.14.5 Testing & validatie

(Geautomatiseerde) vulnerability scans en/of gerichte penetratietests worden herhaald om zeker te stellen dat een eerder gevonden kwetsbaarheid is verholpen en er geen nieuwe issues zijn ontstaan.

5.14.6 Rapportage & compliance

- Relevante stakeholders, zoals IT-management, CISO en compliance officer worden regelmatig van rapportages voorzien over de status van kwetsbaarheden, de genomen maatregelen en de eventuele restrisico's.
- Eventuele bevindingen die de naleving van wettelijke en regulatieve eisen (zoals AVG of NIS2) raken, worden expliciet opgenomen in deze rapportages.
- Als er sprake is van meldplichten (bijvoorbeeld bij een datalek of volgens NIS2) zorgen wij voor een juiste, tijdige melding bij de desbetreffende toezichthouders of autoriteiten.

5.14.7 Evaluatie & continue verbetering

- Het volledige threat & vulnerabilitymanagementproces wordt periodiek geëvalueerd, bijvoorbeeld na een groot beveiligingsincident of op vaste (half)jaarlijkse momenten.
- Op basis van deze evaluaties worden de procedures, tooling en trainingsprogramma's aangepast. Zo blijven we anticiperen op veranderende dreigingen en nieuwe compliance-eisen.
- De pentest-strategie wordt regelmatig herzien, zodat er tijdig ingespeeld wordt op opkomende kwetsbaarheden en de algehele security weerbaarheid van onze organisatie voortdurend verbeteren.

5.15 Patchmanagement

Met patchmanagement verhelp je kwetsbaarheden in systemen, applicaties en hardware. Het doel is om de beveiliging, stabiliteit en prestaties van IT-omgevingen te waarborgen door het tijdig testen en implementeren van patches.

Hiervoor neemt OMO de volgende maatregel:

- OMO heeft een proces voor het inrichten van patchmanagement.

Verantwoordelijkheden:

- De Raad van Bestuur is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving patchmanagement.
- De changemanager is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving patchmanagement.
- De systeemeigenaar is verantwoordelijk voor tijdig testen en implementeren van patches.

5.16 Logging

Loggegevens bieden inzicht in de activiteiten van systemen en spelen een sleutelrol bij het detecteren, onderzoeken en voorkomen van beveiligingsincidenten.

Om loggegevens vast te leggen neemt OMO de volgende maatregel:

- OMO heeft een procesbeschrijving voor het vastleggen van loggegevens binnen systemen.

Verantwoordelijkheden:

- De raad van Bestuur is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving voor logging.
- De teamleider ICT is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving voor logging.

5.17 Digitaal sleutelbeheer

OMO gebruikt encryptie voor de volgende doeleinden:

- Bescherming van vertrouwelijke gegevens: Door het toepassen van sterke versleutelingstechnieken bij opslag, verzending en verwerking van gegevens.
- Verificatie van identiteit: Gebruik van cryptografische methoden zoals digitale handtekeningen en certificaten om betrouwbare communicatie te waarborgen.
- Waarborgen van gegevensintegriteit: Detecteren van wijzigingen in gegevens.

Om encryptie toe te passen treft OMO de volgende maatregel:

- OMO hanteert een procesbeschrijving voor het beheer van digitale sleutels.

Verantwoordelijkheden:

- De teamleider ICT is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving digitaal sleutelbeheer.
- De Key administrator (ICT adviseur) is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving voor digitaal sleutelbeheer.

5.18 Informatiebeveiligingsverslag (IB-verslag)

Elk jaar levert de Functionaris Informatie Beveiliging een informatiebeveiligingsverslag op aan de schoolleider. Dit verslag gaat ook naar de CISO en de Privacyofficer van de vereniging. Dit verslag wordt mede gebaseerd op de resultaten van de zelfevaluatie o.b.v. het IB-normenkader, de verbeteracties, periodieke controles en audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen maatregelen), bewustwordingscampagnes (en de effecten daarvan) en andere initiatieven die de afgelopen periode hebben plaatsgevonden. In dit verslag wordt ook de ambitie voor de komende periode op het gebied van informatiebeveiliging opgenomen.
Schoolleiders gebruiken dit verslag om te rapporteren (op schoolniveau) aan de RvB. De CISO en de privacyofficer van de vereniging rapporteren o.b.v. deze verslagen op verenigingsniveau naar de RvB. In indicatoren voor jaargesprekken van de scholen met de RvB zijn de scores vanuit de zelfevaluatie normenkader en de awarenesstooling opgenomen.

6 Uitgangspunten privacy

Het algemene uitgangspunt in dit IBP-beleid is dat persoonsgegevens in overeenstemming met de AVG en gerelateerde wet- en regelgeving op zorgvuldige wijze worden verwerkt. Om aan dit uitgangspunt te voldoen verwerkt OMO persoonsgegevens in overeenstemming met de privacyvuistregels die in verderop in dit hoofdstuk worden uiteengezet. OMO treft verdiepende maatregelen om de beleidsthema's in dit IBP-beleid in te vullen.

Persoonsgegevens

Persoonsgegevens zijn gegevens die direct of indirect over iemand gaan en dus naar een persoon te herleiden zijn, zoals een naam of e-mailadres. Naast gewone persoonsgegevens - denk aan contactgegevens en onderwijsnummers - onderscheidt de AVG bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens. Daarnaast bestaat een categorie 'gevoelige' persoonsgegevens die niet expliciet in de AVG is benoemd. Dit zijn persoonsgegevens die vanwege hun aard privacygevoelig zijn en daarom extra bescherming verdienen.

- **Bijzondere persoonsgegevens** zijn gegevens die te maken hebben met bijvoorbeeld ras of etnische afkomst, gezondheid, religie of seksueel gedrag. De verwerking van deze gegevens is verboden, tenzij een wettelijke uitzondering bestaat zoals toestemming van de betrokkene.
- **Strafrechtelijke gegevens** zijn gegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. De verwerking van deze gegevens is ook verboden, tenzij hiervoor een wettelijke uitzondering geldt.
- **Gevoelige persoonsgegevens** zijn gegevens die een groter privacyrisico vormen dan gewone persoonsgegevens. Denk aan financiële gegevens, burgerservicenummers (BSN), beoordelingen of gegevens van kwetsbare leerlingen.

NB: Nummers ter identificatie van een persoon, zoals het BSN, mogen alleen worden gebruikt voor specifieke doeleinden die in de wet zijn vastgelegd. Een onderwijsnummer (persoonsgebonden nummer) is gelijk aan het BSN.

Privacyvuistregels

Bij het verwerken van persoonsgegevens houdt OMO rekening met onderstaande basisprincipes. Door deze basisprincipes te volgen zorgen we ervoor dat we kunnen voldoen aan de AVG.

1. **We verwerken persoonsgegevens rechtmatig en transparant**

OMO verzamelt en gebruikt persoonsgegevens op een eerlijke en transparante manier. Persoonsgegevens worden alleen verwerkt als daarvoor een wettelijke grondslag bestaat in de AVG. We leggen altijd duidelijk uit waarom we bepaalde gegevens nodig hebben, wat we ermee doen en hoe lang we deze gegevens bewaren. Daarom informeren we ouders en leerlingen tijdig over het gebruik van hun persoonsgegevens, via een transparante privacyverklaring. Dit gebeurt bijvoorbeeld op het moment van inschrijving van een leerling.

2. We verwerken persoonsgegevens voor specifieke doeleinden

OMO verwerkt persoonsgegevens alleen wanneer vooraf de specifieke doeleinden voor de verwerking zijn bepaald. Deze doeleinden worden vastgelegd. Persoonsgegevens worden niet voor andere, niet-verenigbare, doelen verwerkt. We zullen dus niet persoonsgegevens verzamelen omdat die wellicht ooit van pas gaan komen. We doen dit alleen met vooraf bepaalde, duidelijke en gerechtvaardigde doelen, zoals het plannen van onderwijs en communiceren met leerlingen en ouders over de voortgang en schoolactiviteiten.

3. We verwerken alleen noodzakelijke persoonsgegevens

OMO verzamelt alleen persoonsgegevens die noodzakelijk zijn voor het doel waarvoor ze worden verwerkt. We vragen dus niet om meer gegevens dan we daadwerkelijk nodig hebben en hanteren hierbij het uitgangspunt ‘zo min mogelijk’. We onderzoeken altijd of we met minder gegevens of enkel met anonieme gegevens kunnen werken. Zo vragen we bij de inschrijving van een leerling alleen om de gegevens die relevant zijn voor het kunnen bieden van onderwijs en bewaren we geen overbodige gegevens die niet nodig zijn voor onze schoolactiviteiten.

4. We zorgen dat persoonsgegevens juist en actueel zijn

OMO treft maatregelen om ervoor te zorgen dat persoonsgegevens correct en actueel zijn. Onjuiste of achterhaalde gegevens worden geactualiseerd of verwijderd. Leerlingen en ouders kunnen op een laagdrempelige manier doorgeven dat persoonsgegevens incorrect zijn en/of gewijzigd moeten worden. Onze processen en systemen worden zo ingericht dat de juistheid van gegevens zoveel mogelijk wordt afgedwongen en gecontroleerd.

5. We bewaren persoonsgegevens niet langer dan nodig

OMO bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor ze zijn verzameld. Zodra gegevens niet meer nodig zijn, worden ze verwijderd of geanonimiseerd. We houden ons hierbij aan vooraf vastgestelde bewaartermijnen. Zo wordt het leerlingendossier (inclusief rapporten en schoolprestaties) na uitschrijving van een leerling niet langer bewaard dan nodig is voor administratieve en onderwijsdoeleinden en dus zo spoedig mogelijk verwijderd, in ieder geval binnen 2 jaar na uitschrijving.

6. We zorgen voor een passende bescherming van persoonsgegevens

We kunnen de privacy van leerlingen, ouders en medewerkers alleen goed beschermen als we op een veilige manier met hun persoonsgegevens omgaan. We zijn daarom verantwoordelijk voor het treffen van passende technische en organisatorische beveiligingsmaatregelen. Die maatregelen moeten ervoor zorgen dat de persoonsgegevens op een passende wijze worden beveiligd en worden beschermd tegen verlies, vernietiging, beschadiging of onrechtmatige verwerking. Dit doen we bijvoorbeeld door het gebruik van veilige systemen voor de opslag van leerlinggegevens en het opleiden van personeel in het veilig omgaan met gevoelige gegevens.

7. We kunnen aantonen dat we voldoen aan de AVG

We zijn verantwoordelijk voor het naleven van bovengenoemde vuistregels en kunnen daarmee aantonen dat we voldoen aan de belangrijkste uitgangspunten van de AVG. Dit doen we bijvoorbeeld door het bijhouden van een verwerkingsregister en het uitvoeren van *Data Protection Impact Assesments* (DPIA's) voor gegevensverwerkingen met een hoog privacyrisico.

8. We kunnen ons ethisch verantwoorden

Bij het beoordelen van verwerkingen van persoonsgegevens houdt OMO niet alleen rekening met de vereisten uit de AVG ('*mogen we dit?*'), maar nadrukkelijk ook met ethische aspecten ('*willen we dit*?). Het gaat hierbij dus niet om de vraag of we iets 'mogen' of 'kunnen', maar juist om de vraag of we iets zouden moeten 'willen' als school. Ethische aspecten spelen in het bijzonder een rol bij verwerkingen die privacyrisico's kunnen opleveren, bijvoorbeeld bij het gebruik van meekijksoftware of schermcontroles. Dit moet ook worden bezien vanuit een ethisch afwegingskader. We stellen ons dan ook eerst de vraag of we het kunnen uitleggen aan leerlingen en ouders.

7 Beleidsthema's privacy

7.1 Verwerkingsregister

OMO heeft maatregelen getroffen om aantoonbaar te voldoen aan de eisen uit de AVG. Dit houdt onder meer in dat OMO kan aantonen dat de verwerking van persoonsgegevens voldoet aan de uitgangspunten uit de AVG. OMO geeft onder meer invulling aan haar verantwoordingsplicht door een overzicht bij te houden met informatie over de persoonsgegevens die zij verwerkt. Dit heet het verwerkingsregister. Dit register bevat bijvoorbeeld informatie over de leerlingenadministratie of het HR-systeem. Het bijhouden van het verwerkingsregister zorgt voor een goed overzicht van welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt. Het register stelt OMO in staat te voldoen aan haar verantwoordingsplicht.

Het verwerkingsregister bevat van afzonderlijke verwerkingsactiviteiten informatie over onder meer de doeleinden voor de verwerking, de toepasselijke grondslag onder de AVG, een beschrijving van de betrokkenen, een beschrijving van de persoonsgegevens, de toepasselijke bewaartermijnen en de ontvangers waarmee persoonsgegevens worden gedeeld. Zowel de scholen als het OMO-bureau verwerken alle activiteiten waarbij persoonsgegevens worden verwerkt in het verwerkingsregister.

7.1.1 Legitiem doel en doelbinding

Persoonsgegevens worden alleen verwerkt als een specifiek, vooraf bepaald doel is vastgesteld door OMO. Dit doel moet duidelijk en in begrijpelijke taal aan de betrokkenen worden uitgelegd. Persoonsgegevens mogen niet voor andere doeleinden worden gebruikt.

OMO verwerkt persoonsgegevens om haar verplichtingen als onderwijsinstelling na te kunnen komen. Het schoolbestuur verwerkt persoonsgegevens in de eerste plaats om onderwijs te kunnen bieden aan haar leerlingen en om activiteiten die hieraan ondersteunend zijn te kunnen uitvoeren. Hierbij valt te denken aan verwerkingen in het kader van het aanmeldproces, om te communiceren met leerlingen en ouders/verzorgers, het bijhouden van de leerlingenadministratie, het maken van roosters en om de voortgang bij te houden. Ook verwerkt het schoolbestuur persoonsgegevens van haar medewerkers in haar rol als werkgever. OMO verwerkt bij deze werkzaamheden verschillende (categorieën) persoonsgegevens, waaronder contactgegevens, naam, geboortedatum en gegevens betreffende de aard en het verloop van het onderwijs. OMO verwerkt deze persoonsgegevens op basis van

grondslagen uit de AVG, bijvoorbeeld omdat sprake is van een wettelijke taak of verplichting, een gerechtvaardigd belang of op basis van toestemming.

Als gegevens toch voor een ander doel nodig zijn, dan mag dit alleen als dat doel verenigbaar is met het oorspronkelijke doel. Om te bepalen of dit het geval is, moet onder andere worden gekeken naar:

- De relatie tussen het nieuwe en het oorspronkelijke doel.
- De context waarin de gegevens zijn verzameld en de redelijke verwachtingen van de betrokkenen.
- Het soort persoonsgegevens; gevoelige gegevens verdienen extra bescherming.
- De mogelijke gevolgen voor betrokkenen.
- Bescherming van de gegevens, zoals versleuteling of pseudonimiseren.

Voor elke nieuwe verwerking moet OMO de rechtmatigheid, zorgvuldigheid en noodzaak opnieuw beoordelen. De specifieke doeleinden worden voorafgaand aan de verwerking bepaald en vermeld in de privacyverklaring om betrokken te informeren. Ook worden de doeleinden opgenomen in het verwerkingsregister. Voordat gegevens voor een ander doel worden gebruikt, vindt overleg plaats met de privacy officer en indien nodig ook met de functionaris gegevensbescherming.

7.1.2 Grondslag

OMO moet voor iedere verwerking van persoonsgegevens een geldige reden hebben. De AVG noemt dit een grondslag. OMO verwerkt persoonsgegevens alleen op basis van de in de AVG genoemde grondslagen:

- de betrokkene heeft **toestemming** verleend, bijvoorbeeld voor het maken en delen van foto's of video's.
- de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, bijvoorbeeld het verwerken van salaris om de arbeidsovereenkomst met werknemers na te komen.
- de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting,** bijvoorbeeld het delen van salarisinformatie met de Belastingdienst voor de uitvoering van de belastingwetgeving.
- de verwerking is noodzakelijk om **de vitale belangen** van de betrokkene te beschermen, bijvoorbeeld bij een levensbedreigende situatie waarbij het noodzakelijk is dat bepaalde gegevens van een leerling acuut aan hulpverleners moeten worden doorgeven.
- de verwerking is noodzakelijk om uitvoering te geven aan een **taak van algemeen belang**, hierbij gaat het om wettelijk vastgestelde taken en bevoegdheden**.** Zo heeft OMO en haar scholen de wettelijke taak om onderwijs te bieden.
- de verwerking is noodzakelijk voor de behartiging van een **gerechtvaardigd belang** van OMO of van een derde. Denk hierbij aan het verwerken van medewerkersgegevens voor het opstellen van managementrapportages ten behoeve van beleidsontwikkeling of het gebruik van bewakingscamera's op het schoolplein.

De toepasselijke grondslag wordt vooraf vastgesteld, bijvoorbeeld middels een DPIA, en benoemd in de privacyverklaring om betrokken te informeren. Ook wordt de toepasselijke grondslag opgenomen in het verwerkingsregister.

7.2 Informatieplicht

OMO verwerkt persoonsgegevens op een behoorlijke en transparantie manier. Dit is in begrijpelijke taal inzichtelijk voor de betrokkenen. OMO informeert leerlingen en medewerkers voorafgaand aan de gegevensverwerking op transparante wijze via een duidelijke privacyverklaring. Deze privacyverklaring wordt gepubliceerd op de website. Daarnaast informeert de school medewerkers en sollicitanten ook via een aparte privacyverklaring. Hiermee zorgt

OMO ervoor dat betrokkenen weten welke persoonsgegevens worden verwerkt en voor welke doeleinden dit gebeurt. Ook zijn ze op de hoogte van de rechten die ze hebben.

Wordt gebruikt gemaakt van geautomatiseerde besluitvorming of profilering? Dan gelden extra strenge regels, ook op het gebied van transparantie. Dat betekent onder andere dat medewerkers en leerlingen goed moeten worden geïnformeerd over het gebruik hiervan en duidelijk moet worden uitgelegd op basis van welke criteria het besluit tot stand is gekomen. Ook moet de mogelijkheid bestaan een nieuw besluit te nemen waarbij een mens de gegevens beoordeelt. Op die manier beschermen we medewerkers en leerlingen tegen onrechtmatige verwerking.

7.3 Toestemming

Bij het gebruik van toestemming als grondslag gelden een aantal voorwaarden:

- Toestemming moet op een begrijpelijke en toegankelijke manier worden gevraagd, in duidelijke taal en niet verborgen in algemene voorwaarden of lange teksten.
- Toestemming moet vrijwillig worden gegeven en moet ook weer gemakkelijk ingetrokken kunnen worden.
- OMO moet kunnen aantonen dat toestemming is verkregen, bijvoorbeeld door logs of ondertekende formulieren.
- Voor kinderen onder de 16 jaar moet een wettelijke vertegenwoordiger toestemming geven. Dit geldt ook voor personen onder curatele, bewind of mentorschap. OMO verifieert of deze vertegenwoordiger daadwerkelijk toestemming heeft gegeven.

Leerlingen (of hun wettelijke vertegenwoordigers) worden in bepaalde situaties om toestemming gevraagd. Denk aan de situatie dat OMO foto's of video's van leerlingen maakt en publiceert. Dit mag alleen als de school vooraf toestemming heeft verkregen. Omdat een gezagsrelatie bestaat tussen OMO en haar leerlingen en medewerkers, moet goed worden beargumenteerd waarom toestemming in specifieke gevallen in vrijheid kan worden gegeven. OMO gaat daarom terughoudend om met het gebruik van deze grondslag. Voordat toestemming als grondslag wordt gebruikt, vindt overleg plaats met de privacy officer en indien nodig ook met de functionaris gegevensbescherming.

7.4 Privacy by design en privacy by default

Privacy by design betekent dat OMO bij de ontwikkeling, het ontwerp, de selectie en het gebruik van toepassingen, diensten en producten zo vroeg mogelijk rekening houdt met privacyrisico's en passende waarborgen inbouwt om de privacy van betrokkenen te beschermen. Neemt OMO bijvoorbeeld een leerlingvolgsysteem in gebruik? Dan moet in een vroeg stadium al worden nagedacht over passende toegangsbeperkingen. Leraren horen alleen inzicht te krijgen in de noodzakelijke gegevens van hun eigen leerlingen. *Privacy by default* betekent dat de standaardinstellingen van een product, dienst of proces op de meest privacyvriendelijke instelling staan. Maakt OMO bijvoorbeeld een profiel aan op sociale media? Dan mag dit profiel niet standaard openbaar zichtbaar zijn.

Hiermee zorgt OMO ervoor dat zo vroeg mogelijk rekening wordt gehouden met privacybeginselen en op die manier privacyrisico's tijdig worden gemitigeerd.

7.4.1 Dataminimalisatie

OMO verzamelt alleen gegevens die noodzakelijk zijn voor het doel dat voorafgaand aan de verwerking is vastgesteld. De verzamelde gegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn. Hiermee voorkomt OMO dat te veel gegevens worden verwerkt. Bij de aanmelding van een leerling verzamelt OMO bijvoorbeeld alleen de informatie die nodig is om de leerling op de juiste manier in te schrijven. Denk aan naam, geboortedatum, adres en contactgegevens van ouders/verzorgers. Extra informatie, zoals het beroep van de ouders, is niet relevant voor de

inschrijving en hoort daarom niet te worden verzameld. Daarnaast moet de verwerking van persoonsgegevens op de minst ingrijpende wijze plaatsvinden. Als het beoogde doel op een privacyvriendelijkere manier kan worden bereikt, dan kiest OMO hiervoor. Op deze manier voldoet OMO eveneens aan de principes van *privacy by design*.

7.5 Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld. Dit gebeurt in overeenstemming met het bewaar- en vernietigingsbeleid van OMO. Na het verlopen van de toepasselijke bewaartermijnen zorgt OMO ervoor dat persoonsgegevens tijdig worden vernietigd (of geanonimiseerd). Hierdoor worden persoonsgegevens beter beschermd tegen onnodige verwerking en datalekken. Zo worden bijvoorbeeld overzichten van schoolprestaties en rapporten uiterlijk tot 2 jaar na uitschrijving van een leerling bewaard. Het schooladvies wordt tot uiterlijk 5 jaar na uitschrijving van een leerling bewaard.

7.6 Afhandelen van datalekken

Voorbeelden van datalekken zijn een gestolen laptop, een verloren usb-stick, of een e-mail met persoonsgegevens die naar de verkeerde persoon is verstuurd. Datalekken moeten direct worden gemeld via YourSafetyNet en geregistreerd in het interne register voor beveiligingsincidenten en datalekken. Risicovolle datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens en ook aan de betrokkenen als het datalek waarschijnlijk een hoog risico voor hen oplevert. De privacy officer beoordeelt of zo'n melding nodig is. Dit gebeurt als het nodig is in samenspraak met de functionaris gegevensbescherming.

7.7 Data Protection Impact Assessment

Voor elke nieuwe verwerking van persoonsgegevens, bijvoorbeeld een nieuw proces, technologie of applicatie, controleert OMO of de privacybeginselen uit de AVG worden nageleefd. Bij verwerkingen met een hoog privacyrisico wordt eerst een *Data Protection Impact Assessment* (DPIA) uitgevoerd. Een DPIA brengt in kaart hoe groot de kans is dat de privacy van betrokkenen wordt geschaad, waar de risico's liggen en welke gevolgen dit kan hebben. Op basis van de uitkomsten van de DPIA neemt OMO maatregelen om deze risico's te mitigeren.

7.8 Uitwisseling persoonsgegevens

Een verwerker is een partij die in opdracht van OMO persoonsgegevens verwerkt, zoals een leverancier van een leerlingadministratiesysteem. Als OMO een verwerker inschakelt om persoonsgegevens te verwerken, dan worden privacyafspraken vastgelegd in een verwerkersovereenkomst. Bepaalt OMO samen met één of meerdere partijen het doel en middelen voor de verwerking van persoonsgegevens? Dan is sprake van een zogenaamde gezamenlijke verwerkingsverantwoordelijkheid. In dat geval worden ook contractuele afspraken gemaakt rondom de zorgvuldige en veilige verwerking van gegevens.

Persoonsgegevens kunnen ook beschikbaar worden gesteld aan partijen die niet als verwerkers worden aangemerkt, maar als ‘derden’. Deze derden verwerken persoonsgegevens niet in opdracht van een verwerkingsverantwoordelijke, maar voor hun eigen doel. Een verwerkersovereenkomst is daarom ook niet nodig, maar er moet wel een grondslag bestaan om de persoonsgegevens te delen. Denk aan de situatie waarin OMO gegevens over medewerkers deelt met de Belastingdienst ten behoeve van de loonaangifte. De Belastingdienst verwerkt deze gegevens voor haar eigen wettelijke doeleinden en handelt niet als verwerker.

Gegevensverwerking buiten de EER

Schakelt OMO een verwerker in uit een land buiten de Europese Economische Ruimte (EER) dat geen passend beschermingsniveau biedt? Dan gelden aanvullende voorwaarden. Bij een gegevensdeling buiten de EER moeten namelijk (juridische, technische en organisatorische) waarborgen zijn genomen om het beschermingsniveau ook buiten de EER te laten voldoen aan de AVG, zodat de persoonsgegevens voldoende beschermd blijven. Om dit te bereiken is meer nodig dan alleen het sluiten van een verwerkersovereenkomst. In dat geval maakt OMO gebruik van de Europese modelcontracten, de zogenaamde 'Standard Contractual Clauses', en neemt OMO aanvullende risicogebaseerde beveiligingsmaatregelen. Ook vindt voorafgaand aan de gegevensdeling afstemming plaats met de privacy officer en afdeling informatiebeveiliging om te beoordelen of de getroffen maatregelen voldoende zijn.

NB: De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die als verwerkers in opdracht van de school persoonsgegevens verwerken.

7.9 Rechten van betrokkenen

Betrokkenen hebben op grond van de AVG recht op controle op de verwerking van hun persoonsgegevens. Een betrokkene kan onder andere gebruikmaken van het recht op inzage, rectificatie, verwijdering en bezwaar. Leerlingen, leraren en andere medewerkers kunnen een verzoek tot uitoefening van deze rechten indienen. In het protocol inzageverzoeken staat op welke manier een verzoek kan worden ingediend.Ook hebben betrokkenen het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

OMO draagt er zorg voor dat de informatie over het uitoefenen van deze rechten op een transparante manier is verstrekt aan betrokkenen via een privacyverklaring. OMO zal binnen de wettelijke termijnen, uiterlijk binnen één maand, schriftelijk reageren op het verzoek. In uitzonderlijke situaties kan de reactietermijn worden verlengd, maar dan wordt dit wel binnen een maand gecommuniceerd. Voor AVG-verzoeken geldt een identificatieplicht, zodat de identeit van de verzoeker kan worden vastgesteld. Hiertoe kan OMO om extra informatie verzoeken, maar zal hierbij terughoudend zijn met het verzoeken om een kopie identiteitsbewijs.

Binnen OMO zijn de scholen zelf verantwoordelijk voor het afhandelen van de rechten van betrokkenen. Inzageverzoeken op school worden gecoordineerd en begeleid door de privacy-contactpersoon die zo nodig overlegt met de privacy officer. Ontvangen inzageverzoeken worden door de school centraal geregistreerd (doorgegeven aan de privacy officer). De FG adviseert over de inzageverzoeken en reikwijdte van de verzoeken.

8 Verantwoording informatiebeveiliging en privacy beleid

8.1 Naleving AVG

Er vindt toezicht plaats door OMO op de naleving van de normen uit dit beleid. Van belang is dat leidinggevenden hun verantwoordelijkheid nemen en medewerkers aanspreken in geval van tekortkomingen. OMO besteedt in dit verband actief aandacht aan privacy bij de aanstelling van medewerkers, tijdens functioneringsgesprekken en via bewustwordingscampagnes.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan OMO de betrokken verantwoordelijke medewerkers maatregelen opleggen binnen de kaders van de CAO en toepasselijke wetgeving.

Voor toezicht op de naleving van de AVG vervult de functionaris gegevensbescherming (FG) een belangrijke rol. De FG kan bijvoorbeeld informatie verzamelen over gegevensverwerkingen en beoordelen of deze aan de AVG voldoen. Ook kan de FG adviezen en aanbevelingen verschaffen aan OMO.

8.2 Naleving IBP-normenkader Funderend Onderwijs

Er vindt toezicht plaats op de naleving van het normenkader IBP voor het funderend onderwijs op de naleving van alle normen. Ook hierbij besteedt OMO in dit verband actief aandacht aan informatiebeveiliging, en privacy, bij de aanstelling van medewerkers, tijdens functioneringsgesprekken en via bewustwordingscampagnes.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan OMO de betrokken verantwoordelijke medewerkers maatregelen opleggen binnen de kaders van de CAO en toepasselijke wetgeving.

Als hulpmiddel gebruiken we hiervoor een Governance en Compliance tool waarin iedere school, en het OMO bureau, de voortgang, en bewijslast, kan administreren. Op basis van deze bewijslasten zullen er audits plaats gaan vinden bij alle scholen.

Binnen dit normenkader zullen de security officer en privacy officer gezaamlijk optrekken om de scholen hierin mee te nemen en de scholen te begeleiden zodat de scholen op 1 januari 2027 voldoen aan volwassenheidsniveau 3.

8.3 Rapportage

OMO heeft de verantwoordelijkheid om het informatie en privacy beleid formeel goed te keuren en te monitoren of het beleid door de organisatie wordt toegepast. Jaarlijiks wordt hierover gerapporteerd in het jaarverslag Informatiebeveiliging en Privacy.

8.4 Beleidsherziening

Het informatiebeveiliging en privacy beleid wordt door OMO eenmaal per jaar getoetst en indien nodig herzien. Bij een substantiële wijziging van dit beleid of in geval van belangrijke ontwikkelingen of veranderingen in wet- en regelgeving, volgt er indien nodig een beleidswijziging.

Bijlagen (uitvoeringsbeleid: nog op te stellen)

- Interne privacyverklaring
- Externe privacyverklaring
- Bewaar- en vernietigingsbeleid
- Beleid inzageverzoeken
- Beleid DPIA
- Beleid cameratoezicht
- IAM beleid
- ICT Business Continuity Plan
- ICT Crisis Plan