1. Doel en reikwijdte

1.1 Doel

Dit privacybeleid beschrijft op welke wijze **Basisschool De Tweestroom** en het bevoegd gezag **SPO De Sprong** omgaan met persoonsgegevens van leerlingen, ouders/verzorgers, medewerkers en andere betrokkenen. Het beleid heeft tot doel te waarborgen dat persoonsgegevens binnen de schoolorganisatie op een rechtmatige, behoorlijke, transparante en zorgvuldige wijze worden verwerkt, in overeenstemming met de Algemene verordening gegevensbescherming (AVG) en overige toepasselijke wet- en regelgeving.

Met dit beleid wordt beoogd:

- persoonsgegevens uitsluitend te verwerken voor duidelijk omschreven en gerechtvaardigde doeleinden;
- niet meer persoonsgegevens te verwerken dan noodzakelijk is voor het beoogde doel;
- persoonsgegevens juist, actueel en passend beveiligd te houden;
- betrokkenen duidelijk te informeren over de wijze waarop hun persoonsgegevens worden verwerkt;
- de rechten van betrokkenen zorgvuldig en tijdig te waarborgen;
- aantoonbaar invulling te geven aan de verantwoordingsplicht.

Dit beleid vormt daarmee het kader voor een zorgvuldige en consistente omgang met persoonsgegevens binnen de schoolorganisatie.

1.2 Reikwijdte ten aanzien van betrokkenen

Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens waarvoor de school en/of het bevoegd gezag verwerkingsverantwoordelijke is, dan wel waarvoor persoonsgegevens onder verantwoordelijkheid van de school worden verwerkt.

Het beleid heeft in ieder geval betrekking op persoonsgegevens van:

- leerlingen;
- ouders, verzorgers en wettelijke vertegenwoordigers;
- medewerkers, waaronder vaste en tijdelijke medewerkers;
- stagiairs, vrijwilligers en invalkrachten;
- sollicitanten;
- leveranciers, opdrachtnemers en andere externe contacten;
- samenwerkingspartners, zoals organisaties op het gebied van kinderopvang, jeugdhulp, zorg en ondersteuning, voor zover daarbij persoonsgegevens worden verwerkt.

Onder persoonsgegevens wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

1.3 Reikwijdte ten aanzien van verwerkingen

Dit beleid is van toepassing op alle vormen van verwerking van persoonsgegevens binnen de schoolorganisatie, ongeacht of deze verwerking digitaal, op papier of op andere wijze plaatsvindt.

Daaronder vallen onder meer:

- verwerkingen in administratieve systemen, leerlingvolgsystemen, personeels- en HR-systemen, e-mailomgevingen, cloudtoepassingen en digitale leermiddelen;
- papieren dossiers, formulieren en overige documentatie;
- communicatie via websites, ouderportalen, nieuwsbrieven en andere schoolgerelateerde kanalen;
- verwerking van persoonsgegevens op apparaten die door de school beschikbaar zijn gesteld;
- verwerking van persoonsgegevens in het kader van thuiswerken of mobiel werken;
- uitwisseling van persoonsgegevens met derden, voor zover deze plaatsvindt in het kader van onderwijs, begeleiding, bedrijfsvoering, samenwerking of wettelijke verplichtingen.

Het beleid ziet daarmee op de gehele levenscyclus van persoonsgegevens, waaronder het verzamelen, vastleggen, opslaan, raadplegen, gebruiken, delen, wijzigen, archiveren en verwijderen van gegevens.

1.4 Doeleinden van verwerking

Persoonsgegevens worden uitsluitend verwerkt voor zover dat noodzakelijk is voor de uitvoering van de taken van de school en het bevoegd gezag. Het betreft in ieder geval verwerkingen die nodig zijn voor:

- het verzorgen van onderwijs;
- de begeleiding en ondersteuning van leerlingen;
- het volgen van de ontwikkeling en voortgang van leerlingen;
- de communicatie met ouders/verzorgers;
- het voeren van de leerlingadministratie en personeelsadministratie;
- de organisatie van veiligheid, ondersteuning en zorg binnen de school;
- de uitvoering van arbeidsrelaties, stageplaatsen en vrijwilligerswerk;
- het voldoen aan wettelijke verplichtingen en verantwoordingsverplichtingen;
- het waarborgen van de continuïteit, beveiliging en betrouwbaarheid van systemen en informatievoorziening.

Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met deze doeleinden, tenzij daarvoor een afzonderlijke wettelijke grondslag bestaat.

1.5 Juridisch kader

Dit beleid is gebaseerd op de Algemene verordening gegevensbescherming (AVG) en andere relevante wet- en regelgeving die van toepassing is op het primair onderwijs en op de verwerking van persoonsgegevens binnen de schoolorganisatie.

Bij de verwerking van persoonsgegevens worden de geldende wettelijke kaders steeds in onderlinge samenhang toegepast. Indien een verwerking noodzakelijk is op grond van een wettelijke verplichting of ter uitvoering van een publieke taak, vindt deze verwerking plaats binnen de grenzen van proportionaliteit, subsidiariteit en zorgvuldigheid.

1.6 Uitgangspunt van zorgvuldige en aantoonbare naleving

Privacybescherming maakt integraal onderdeel uit van goed onderwijsbestuur en een professionele schoolorganisatie. Dit betekent dat zorgvuldig omgaan met persoonsgegevens niet uitsluitend een juridische verplichting is, maar ook een vast onderdeel vormt van de dagelijkse praktijk, de inrichting van processen en het handelen van medewerkers.

De schoolorganisatie geeft hieraan uitvoering door:

- beleid, procedures en werkafspraken vast te stellen;
- verantwoordelijkheden binnen de organisatie helder te beleggen;
- medewerkers te instrueren over het zorgvuldig verwerken van persoonsgegevens;
- verwerkingen vast te leggen in een verwerkingsregister;
- betrokkenen adequaat te informeren;
- passende technische en organisatorische beveiligingsmaatregelen te treffen;
- periodiek te toetsen of de werkwijze nog voldoet aan wetgeving en praktijk.

1.7 Samenhang met andere documenten

Dit beleid is een overkoepelend kaderdocument. De nadere uitwerking van specifieke onderwerpen is opgenomen in aanvullende documenten en procedures, waaronder:

- de privacyverklaring;
- het verwerkingsregister;
- het informatiebeveiligingsbeleid;
- de procedure voor de afhandeling van rechten van betrokkenen;
- het datalekprotocol;
- het protocol beeldmateriaal;
- de bewaartermijnenmatrix;
- verwerkersovereenkomsten en leveranciersafspraken.

Deze documenten vormen gezamenlijk het privacy- en informatiebeveiligingskader van de organisatie.

1.8 Gelding, vaststelling en evaluatie

Dit beleid geldt voor de gehele schoolorganisatie en voor alle personen die onder verantwoordelijkheid van de school of het bevoegd gezag persoonsgegevens verwerken.

Het beleid wordt vastgesteld door het bevoegd gezag en periodiek geëvalueerd. Indien daartoe aanleiding bestaat, wordt het beleid tussentijds aangepast. Een actualisatie vindt in ieder geval plaats bij:

- wijzigingen in wet- en regelgeving;
- relevante organisatorische veranderingen;
- invoering van nieuwe systemen, processen of verwerkingen;
- bevindingen uit audits, evaluaties, incidenten of adviezen van de Functionaris Gegevensbescherming.

Op deze wijze blijft het beleid actueel, uitvoerbaar en in overeenstemming met de feitelijke praktijk binnen de organisatie.

2. Rollen en verantwoordelijkheden

2.1 Algemeen

Voor een zorgvuldige en rechtmatige verwerking van persoonsgegevens is het noodzakelijk dat binnen de organisatie helder is vastgelegd wie welke verantwoordelijkheden draagt. De verantwoordelijkheid voor privacy en gegevensbescherming ligt niet bij één functionaris בלבד, maar is belegd op verschillende niveaus binnen de organisatie. Iedere rol draagt, binnen de eigen taakuitoefening, bij aan de naleving van de AVG en aan een zorgvuldige omgang met persoonsgegevens.

2.2 Bevoegd gezag

Het bevoegd gezag, **SPO De Sprong**, treedt voor de meeste verwerkingen van persoonsgegevens op als **verwerkingsverantwoordelijke**. Dit betekent dat het bevoegd gezag bepaalt voor welke doeleinden en met welke middelen persoonsgegevens worden verwerkt.

Het bevoegd gezag is in dat kader verantwoordelijk voor:

- het vaststellen van het privacybeleid en aanverwante regelingen;
- het zorgen voor een passende organisatorische inrichting van privacy en informatiebeveiliging;
- het beschikbaar stellen van voldoende middelen, capaciteit en ondersteuning;
- het toezien op naleving van wet- en regelgeving binnen de organisatie;
- het borgen van een adequate verdeling van taken, bevoegdheden en verantwoordelijkheden;
- het aangaan van overeenkomsten met verwerkers en andere externe partijen, voor zover vereist;
- het waarborgen dat de organisatie aantoonbaar kan voldoen aan de verantwoordingsplicht.

Het bevoegd gezag draagt de eindverantwoordelijkheid voor de wijze waarop binnen de organisatie met persoonsgegevens wordt omgegaan.

2.3 Schoolleiding

De schoolleiding van **Basisschool De Tweestroom** is verantwoordelijk voor de uitvoering van het vastgestelde beleid binnen de dagelijkse schoolpraktijk. De schoolleiding draagt er zorg voor dat privacybeleid, procedures en werkafspraken daadwerkelijk worden toegepast in de organisatie en dat medewerkers weten wat van hen wordt verwacht.

De schoolleiding is in het bijzonder verantwoordelijk voor:

- de implementatie van privacybeleid en procedures op schoolniveau;
- het bevorderen van naleving door medewerkers;
- het inbedden van privacy en informatiebeveiliging in werkprocessen;
- het toezien op een zorgvuldige omgang met dossiers, systemen en communicatiemiddelen;
- het zorgen voor passende instructie en begeleiding van medewerkers;
- het tijdig opschalen van privacyvragen, incidenten en risico's naar de daarvoor aangewezen functionarissen;
- het bevorderen van een cultuur waarin datalekken en beveiligingsincidenten direct worden gemeld.

De schoolleiding vervult daarmee een cruciale rol in de vertaalslag van beleid naar uitvoering.

2.4 Functionaris voor Gegevensbescherming

De organisatie beschikt over een **Functionaris voor Gegevensbescherming (FG)**. De FG houdt onafhankelijk toezicht op de toepassing en naleving van de privacywetgeving binnen de organisatie en adviseert over de bescherming van persoonsgegevens.

De FG heeft onder meer de volgende taken:

- informeren en adviseren van bestuur, schoolleiding en medewerkers over hun verplichtingen op grond van de AVG;
- toezien op de naleving van privacywetgeving, intern beleid en werkafspraken;

- adviseren over gegevensbeschermingseffectbeoordelingen (DPIA's);
- fungeren als contactpunt voor de Autoriteit Persoonsgegevens;
- fungeren als intern aanspreekpunt voor privacyvraagstukken, voor zover passend binnen de onafhankelijke toezichtsrol.

De FG vervult deze taken in een onafhankelijke positie en ontvangt geen instructies over de wijze waarop deze toezichthoudende taak wordt uitgevoerd.

In dit beleid worden de actuele contactgegevens van de FG opgenomen:

- Naam: [...]
- Organisatie: [...]
- E-mailadres: [...]
- Telefoonnummer: [...]

2.5 Privacycoördinator / IBP-coördinator

Ter ondersteuning van de dagelijkse uitvoering kan binnen de organisatie een privacycoördinator en/of IBP-coördinator zijn aangewezen. Deze rol ondersteunt de praktische organisatie van privacy en informatiebeveiliging en vormt veelal het eerste aanspreekpunt binnen de interne organisatie voor operationele privacyzaken.

De privacycoördinator / IBP-coördinator kan onder meer belast zijn met:

- het beheren en actualiseren van het verwerkingsregister;
- het beheren van het datalekregister;
- het coördineren van rechtenverzoeken van betrokkenen;
- het ondersteunen bij DPIA's en risicobeoordelingen;
- het beheren van documentatie, formats en procedures;
- het signaleren van verbeterpunten in processen en werkwijzen;
- het ondersteunen bij bewustwording en instructie van medewerkers;
- het onderhouden van afstemming met ICT, schoolleiding en FG.

Indien deze rol is ingericht, worden taken, bevoegdheden en verantwoordelijkheden nader intern vastgelegd.

2.6 ICT-beheer en informatiebeveiliging

De functionaris of afdeling die verantwoordelijk is voor ICT-beheer en informatiebeveiliging draagt zorg voor de technische en operationele beveiliging van systemen en gegevensverwerking binnen de organisatie.

Daaronder vallen onder meer:

- het beheer van accounts en toegangsrechten;
- het toekennen, wijzigen en intrekken van autorisaties;
- het beveiligen van systemen, apparaten en netwerken;
- het uitvoeren van updates, patchmanagement en technisch onderhoud;
- het inrichten van back-ups en herstelvoorzieningen;
- het signaleren en onderzoeken van beveiligingsincidenten;
- het ondersteunen bij containment en herstelmaatregelen bij datalekken of beveiligingsincidenten;
- het adviseren over passende technische beveiligingsmaatregelen.

ICT-beheer werkt hierbij samen met de schoolleiding, de privacycoördinator en, waar nodig, de FG.

2.7 Medewerkers

Alle medewerkers van de schoolorganisatie hebben een eigen verantwoordelijkheid bij het zorgvuldig verwerken van persoonsgegevens. Dit geldt voor onderwijzend personeel, onderwijsondersteunend personeel, leidinggevenden, tijdelijke medewerkers en andere personen die in opdracht of onder verantwoordelijkheid van de organisatie werken.

Van medewerkers wordt verwacht dat zij:

- persoonsgegevens uitsluitend verwerken voor zover dat noodzakelijk is voor de uitvoering van hun werkzaamheden;
- vertrouwelijk omgaan met persoonsgegevens;

- de geldende beleidsregels, procedures en werkafspraken naleven;
- zorgvuldig omgaan met accounts, wachtwoorden, systemen en documenten;
- persoonsgegevens niet delen met onbevoegden;
- mogelijke datalekken, beveiligingsincidenten of onregelmatigheden direct melden via de interne procedure;
- deelnemen aan instructies en bewustwordingsactiviteiten op het gebied van privacy en informatiebeveiliging.

Iedere medewerker heeft daarmee een eigen professionele verantwoordelijkheid in het beschermen van persoonsgegevens.

2.8 Stagiairs, vrijwilligers en externen

Ook stagiairs, vrijwilligers, inhuurkrachten en andere externen die onder verantwoordelijkheid van de school werkzaamheden verrichten en daarbij toegang hebben tot persoonsgegevens, zijn gehouden aan dezelfde uitgangspunten van zorgvuldigheid, vertrouwelijkheid en beveiliging.

Voor deze groepen geldt dat:

- zij uitsluitend toegang krijgen tot persoonsgegevens voor zover dat noodzakelijk is voor hun taak;
- zij vooraf worden geïnstrueerd over de geldende privacy- en beveiligingsregels;
- waar nodig aanvullende afspraken worden vastgelegd, bijvoorbeeld in een stageovereenkomst, vrijwilligersverklaring of geheimhoudingsverklaring;
- hun toegang tot systemen en gegevens tijdig wordt aangepast of beëindigd zodra de werkzaamheden eindigen.
-

2.9 Leveranciers en verwerkers

Externe partijen die in opdracht van de organisatie persoonsgegevens verwerken, doen dit uitsluitend op basis van duidelijke afspraken en binnen de grenzen van de toepasselijke wet- en regelgeving.

Indien een externe partij kwalificeert als verwerker, wordt met deze partij een verwerkersovereenkomst gesloten waarin in ieder geval afspraken worden vastgelegd over:

- de aard en duur van de verwerking;
- de doeleinden van de verwerking;
- de beveiligingsmaatregelen;
- geheimhouding;
- inzet van subverwerkers;
- meldingen van datalekken en beveiligingsincidenten;
- controle, verwijdering en teruggave van gegevens.

De verantwoordelijkheid voor een zorgvuldige selectie en aansturing van dergelijke partijen ligt bij het bevoegd gezag, met ondersteuning vanuit de daartoe aangewezen functionarissen.

2.10 Samenwerking en escalatie

Een zorgvuldige naleving van privacywetgeving vereist afstemming tussen bestuur, schoolleiding, privacycoördinatie, ICT-beheer, FG en medewerkers. Daarom geldt binnen de organisatie dat privacyvraagstukken, risico's, incidenten en signalen tijdig worden gedeeld met de juiste functionarissen.

Indien sprake is van twijfel over de rechtmatigheid van een verwerking, een beveiligingsrisico of een mogelijk datalek, wordt dit onverwijld gemeld via de daarvoor vastgestelde interne lijn. Daarbij geldt in algemene zin de volgende escalatiestructuur:

- medewerker naar schoolleiding en/of privacycoördinator;
- privacycoördinator naar ICT en, indien nodig, de FG;
- schoolleiding of privacycoördinator naar het bevoegd gezag bij bestuurlijk relevante risico's of besluiten.

Op deze wijze wordt geborgd dat privacyvraagstukken zorgvuldig, tijdig en op het juiste niveau worden behandeld.

2.11 Slotbepaling

Iedere functionaris en iedere medewerker binnen de organisatie is gehouden om binnen de eigen rol en verantwoordelijkheid bij te dragen aan een rechtmatige, veilige en zorgvuldige verwerking van persoonsgegevens. Heldere taakverdeling, goede samenwerking en tijdige afstemming vormen daarbij de basis.

3. Basisprincipes

3.1 Algemeen

Bij alle verwerkingen van persoonsgegevens handelt de schoolorganisatie in overeenstemming met de uitgangspunten van de Algemene verordening gegevensbescherming (AVG). Deze beginselen vormen de basis voor iedere verwerking van persoonsgegevens binnen de organisatie en zijn richtinggevend voor beleid, inrichting van processen, gebruik van systemen en het dagelijks handelen van medewerkers.

De verwerking van persoonsgegevens vindt uitsluitend plaats indien daarvoor een duidelijke noodzaak bestaat en indien deze verwerking past binnen de taken en verantwoordelijkheden van de school en het bevoegd gezag. Daarbij geldt dat steeds een zorgvuldige afweging wordt gemaakt tussen het doel van de verwerking, de noodzaak daarvan en de impact op de persoonlijke levenssfeer van betrokkenen.

3.2 Rechtmatigheid, behoorlijkheid en transparantie

Persoonsgegevens worden uitsluitend verwerkt indien daarvoor een geldige grondslag bestaat en indien de verwerking op een behoorlijke en zorgvuldige wijze plaatsvindt. De organisatie verwerkt persoonsgegevens niet op een manier die voor betrokkenen onverwacht, misleidend of onredelijk is.

Daarnaast draagt de organisatie er zorg voor dat betrokkenen op duidelijke en begrijpelijke wijze worden geïnformeerd over:

- welke persoonsgegevens worden verwerkt;
- voor welke doeleinden deze gegevens worden verwerkt;
- op basis van welke grondslag de verwerking plaatsvindt;
- met welke partijen gegevens worden gedeeld, indien dat aan de orde is;
- hoe lang persoonsgegevens worden bewaard;
- welke rechten betrokkenen hebben.

Transparantie is een wezenlijk uitgangspunt. Dit betekent dat de organisatie niet alleen rechtmatig handelt, maar ook kan uitleggen op welke wijze en waarom persoonsgegevens worden verwerkt.

3.3 Doelbinding

Persoonsgegevens worden uitsluitend verzameld en verwerkt voor **uitdrukkelijk omschreven, gerechtvaardigde en welbepaalde doeleinden**. Gegevens worden niet verwerkt op een wijze die onverenigbaar is met het oorspronkelijke doel waarvoor zij zijn verkregen, tenzij daarvoor een afzonderlijke wettelijke grondslag bestaat.

Voor de schoolorganisatie betekent dit dat persoonsgegevens alleen worden verwerkt voor zover dat noodzakelijk is voor bijvoorbeeld:

- het verzorgen van onderwijs;
- het begeleiden van leerlingen;
- het voeren van een deugdelijke administratie;
- het ondersteunen van medewerkers in de uitvoering van hun werkzaamheden;
- het voldoen aan wettelijke verplichtingen;
- het waarborgen van de veiligheid, continuïteit en kwaliteit van de organisatie.

Nieuwe of gewijzigde verwerkingen worden vooraf beoordeeld op doel en noodzaak. Wanneer het doel van een verwerking verandert, wordt beoordeeld of die wijziging verenigbaar is met het oorspronkelijke doel en of aanvullende waarborgen of maatregelen nodig zijn.

3.4 Dataminimalisatie

De organisatie verwerkt uitsluitend persoonsgegevens die **toereikend, ter zake dienend en beperkt** zijn tot wat noodzakelijk is voor het doel van de verwerking. Er worden dus niet meer persoonsgegevens verzameld, vastgelegd of gedeeld dan nodig is.

Dit betekent onder meer dat:

- alleen gegevens worden opgevraagd die nodig zijn voor het betreffende proces;

- toegang tot persoonsgegevens wordt beperkt tot personen die deze gegevens voor hun taakuitoefening nodig hebben;
- formulieren, registraties en systemen periodiek worden beoordeeld op overbodige gegevensverwerking;
- geen gegevens worden bewaard of gedeeld “voor het geval dat”, zonder concrete noodzaak of grondslag.
- Dataminimalisatie geldt zowel bij de inrichting van processen als bij het dagelijks gebruik van gegevens door medewerkers.

3.5 Juistheid van gegevens

De organisatie draagt er zorg voor dat persoonsgegevens juist en, waar nodig, actueel zijn. Onjuiste of verouderde gegevens worden zo spoedig mogelijk gecorrigeerd, aangevuld of verwijderd, afhankelijk van de aard van het gegeven en het doel van de verwerking.

Van medewerkers wordt verwacht dat zij zorgvuldig omgaan met het vastleggen van gegevens en bij twijfel of onjuistheden passende actie ondernemen. Dit geldt in het bijzonder voor gegevens in leerlingdossiers, administratieve systemen en personeelsbestanden, omdat onjuiste gegevens gevolgen kunnen hebben voor de begeleiding, besluitvorming of communicatie.

De organisatie faciliteert daarnaast dat betrokkenen gebruik kunnen maken van hun recht op rectificatie, overeenkomstig de daarvoor geldende procedure.

3.6 Opslagbeperking

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor het doel waarvoor zij zijn verzameld of verwerkt, tenzij een wettelijke bewaarplicht of andere rechtmatige grond een langere bewaartermijn vereist.

Binnen de organisatie betekent dit dat:

- per gegevensstroom of verwerkingsdoel bewaartermijnen worden vastgesteld;
- persoonsgegevens na afloop van de bewaartermijn worden verwijderd, vernietigd of, indien passend, geanonimiseerd;

- systemen, mailboxen, netwerklocaties en papieren archieven periodiek worden beoordeeld op gegevens die niet langer bewaard hoeven te worden;
- bewaartermijnen worden vastgelegd in het verwerkingsregister en, waar nodig, in een afzonderlijke bewaartermijnenmatrix.

Opslagbeperking is niet alleen een administratieve verplichting, maar ook een belangrijk middel om privacyrisico's te beperken.

3.7 Integriteit en vertrouwelijkheid

Persoonsgegevens worden op een zodanige wijze verwerkt dat een passende beveiliging is gewaarborgd. Dit omvat bescherming tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging van persoonsgegevens.

De organisatie treft daartoe passende technische en organisatorische maatregelen. Daarbij valt onder meer te denken aan:

- toegangsbeperking op basis van rollen en taken;
- beveiliging van accounts en wachtwoorden;
- gebruik van beveiligde systemen en verbindingen;
- zorgvuldige verzending van persoonsgegevens;
- logging, back-ups en herstelvoorzieningen;
- instructies voor veilig werken, zowel op school als op afstand;
- maatregelen ter voorkoming van onbevoegde inzage, verlies of misbruik.

Vertrouwelijkheid geldt voor iedereen die binnen de organisatie toegang heeft tot persoonsgegevens. Persoonsgegevens worden uitsluitend gedeeld met personen of partijen die daartoe bevoegd zijn en voor zover dat noodzakelijk is voor het doel van de verwerking.

3.8 Verantwoordingsplicht

De organisatie hanteert het uitgangspunt dat zij niet alleen moet voldoen aan de privacyregels, maar dit ook moet kunnen **aantonen**. Daarom worden keuzes, procedures en maatregelen op passende wijze vastgelegd.

De verantwoordingsplicht krijgt onder meer vorm door:

- het vaststellen en onderhouden van privacy- en informatiebeveiligingsbeleid;
- het bijhouden van een actueel verwerkingsregister;
- het vastleggen van rollen, verantwoordelijkheden en procedures;
- het documenteren van datalekken, rechtenverzoeken en relevante afwegingen;
- het sluiten van verwerkersovereenkomsten met externe partijen waar nodig;
- het uitvoeren van controles, evaluaties en waar passend DPIA's;
- het periodiek trainen en informeren van medewerkers.

Door deze werkwijze wordt geborgd dat privacybescherming een aantoonbaar en structureel onderdeel is van de organisatie.

3.9 Need-to-know en zorgvuldige toegang

Binnen de organisatie geldt als uitgangspunt dat persoonsgegevens alleen toegankelijk zijn voor personen die deze gegevens daadwerkelijk nodig hebben voor de uitvoering van hun werkzaamheden. Toegang tot persoonsgegevens wordt daarom beperkt op basis van functie, rol en taak.

Dit betekent dat:

- medewerkers uitsluitend toegang krijgen tot die systemen en dossiers die voor hun werkzaamheden noodzakelijk zijn;
- autorisaties zorgvuldig worden toegekend, gewijzigd en ingetrokken;
- vertrouwelijke gegevens niet onnodig intern worden gedeeld;
- medewerkers terughoudend omgaan met inzage in gegevens van leerlingen, ouders/verzorgers, collega's en andere betrokkenen;
- gegevens niet worden ingezien uit nieuwsgierigheid of buiten de eigen taakuitoefening.

Het beginsel van need-to-know vormt een praktische uitwerking van dataminimalisatie en vertrouwelijkheid.

3.10 Zorgvuldige communicatie en gegevensdeling

Bij het delen of verzenden van persoonsgegevens handelt de organisatie terughoudend en zorgvuldig. Persoonsgegevens worden uitsluitend gedeeld indien daarvoor een duidelijke noodzaak en, waar vereist, een geldige grondslag bestaat.

Daarbij gelden in ieder geval de volgende uitgangspunten:

- persoonsgegevens worden bij voorkeur gedeeld via goedgekeurde en beveiligde communicatiemiddelen;
- verzending naar derden vindt alleen plaats na controle van adressering, inhoud en noodzaak;
- privé-mailadressen, privé-apps en andere niet-goedgekeurde kanalen worden niet gebruikt voor het delen van privacygevoelige gegevens, tenzij hiervoor uitdrukkelijk beleid en passende beveiligingsmaatregelen bestaan;
- bij het delen van persoonsgegevens wordt steeds beoordeeld of de gegevens kunnen worden beperkt, afgeschermd of gepseudonimiseerd;
- mondelinge, schriftelijke en digitale communicatie vindt zodanig plaats dat onbevoegde kennisneming zoveel mogelijk wordt voorkomen.

3.11 Privacy by design en privacy by default

Bij de inrichting van nieuwe processen, systemen, formulieren, digitale toepassingen en werkwijzen wordt privacy vanaf het begin meegenomen. Dit betekent dat al in de ontwerpfase aandacht wordt besteed aan noodzaak, proportionaliteit, beveiliging, bewaartermijnen, toegangsbeperking en transparantie.

Daarnaast wordt het uitgangspunt gehanteerd dat standaardinstellingen privacyvriendelijk zijn ingericht. Alleen die persoonsgegevens die noodzakelijk zijn voor het specifieke doel worden verwerkt, en alleen de personen die toegang nodig hebben, krijgen deze toegang.

Dit beginsel geldt onder meer bij:

- de aanschaf of invoering van nieuwe systemen;
- wijzigingen in digitale leermiddelen;

- het opstellen van formulieren en registraties;
- het inrichten van accounts, rollen en autorisaties;
- het opzetten van nieuwe samenwerkingen of gegevensuitwisselingen.

3.12 Praktische gedragslijn binnen de organisatie

Ter ondersteuning van deze basisprincipes gelden binnen de organisatie de volgende algemene gedragsregels:

- medewerkers verwerken alleen persoonsgegevens die nodig zijn voor hun werkzaamheden;
- persoonsgegevens worden niet gedeeld met onbevoegden;
- schoolgebonden gegevens worden niet via privékanalen verwerkt of opgeslagen, tenzij dat uitdrukkelijk is toegestaan en passend beveiligd is;
- documenten en schermen met persoonsgegevens worden niet onbeheerd toegankelijk achtergelaten;
- twijfel over de rechtmatigheid of zorgvuldigheid van een verwerking wordt tijdig besproken met de schoolleiding, privacycoördinator of andere aangewezen functionaris;
- incidenten en mogelijke datalekken worden direct gemeld volgens de geldende procedure.

3.13 Slotbepaling

De in dit hoofdstuk opgenomen basisprincipes gelden voor alle verwerkingen van persoonsgegevens binnen de organisatie en vormen het normatieve uitgangspunt voor de toepassing van dit beleid. Nadere uitwerking van deze beginselen vindt plaats in procedures, werkafspraken en aanvullende beleidsdocumenten.

4. Rechtsgrondslagen

4.1 Algemeen

Persoonsgegevens worden alleen verwerkt indien daarvoor een geldige rechtsgrond bestaat. Voor iedere verwerking wordt vooraf vastgesteld op welke rechtsgrond deze berust. De school verwerkt geen persoonsgegevens zonder duidelijke wettelijke basis of aantoonbare noodzaak.

4.2 Wettelijke verplichting en publieke taak

Voor een groot deel van de verwerkingen binnen het primair onderwijs geldt dat deze noodzakelijk zijn vanwege een **wettelijke verplichting** of voor de uitvoering van een **taak van algemeen belang**. Dit geldt in het bijzonder voor verwerkingen die samenhangen met:

- de leerlingadministratie;
- inschrijving en uitschrijving;
- het verzorgen van onderwijs;
- het volgen van de ontwikkeling van leerlingen;
- verzuimregistratie;
- bekostiging, verantwoording en toezicht;
- begeleiding en ondersteuning voor zover dit onderdeel is van de onderwijstaak.

Voor deze verwerkingen is in beginsel geen toestemming nodig, omdat de school deze gegevens moet of mag verwerken op grond van haar wettelijke taken.

4.3 Uitvoering van een overeenkomst

Persoonsgegevens kunnen worden verwerkt wanneer dit noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is.

Dit speelt binnen de schoolorganisatie met name bij:

- arbeidsovereenkomsten;
- stageovereenkomsten;
- overeenkomsten met vrijwilligers of opdrachtnemers, voor zover van toepassing;

- overeenkomsten met leveranciers of externe dienstverleners, voor zover het gaat om contact- en contractgegevens van natuurlijke personen.

Alleen gegevens die noodzakelijk zijn voor de uitvoering van de overeenkomst worden verwerkt.

4.4 Gerechtvaardigd belang

In bepaalde gevallen kan een verwerking gebaseerd zijn op een **gerechtvaardigd belang**, mits de belangen of grondrechten van de betrokkene niet zwaarder wegen. Deze grondslag wordt terughoudend toegepast en alleen gebruikt na een zorgvuldige belangenafweging.

Bij toepassing van deze grondslag wordt beoordeeld:

- wat het belang van de school of organisatie is;
- of de verwerking noodzakelijk is voor dat belang;
- welke gevolgen de verwerking heeft voor de betrokkene;
- welke waarborgen worden getroffen om de privacy te beschermen.

De afweging wordt, waar nodig, vastgelegd.

4.5 Toestemming

Indien geen andere passende rechtsgrond van toepassing is, kan verwerking plaatsvinden op basis van **toestemming**. Toestemming wordt alleen gevraagd wanneer deze vrij, specifiek, geïnformeerd en ondubbelzinnig kan worden gegeven.

Toestemming moet daarnaast:

- aantoonbaar zijn vastgelegd;
- op ieder moment kunnen worden ingetrokken;
- los staan van andere voorwaarden of verplichtingen;
- zonder nadelige gevolgen kunnen worden geweigerd of ingetrokken.

De school gebruikt toestemming niet als standaardgrondslag voor verwerkingen die al op een wettelijke verplichting, publieke taak of overeenkomst berusten.

4.6 Beeldmateriaal

Voor het maken en/of publiceren van herkenbaar beeldmateriaal van leerlingen wordt toestemming gevraagd, tenzij sprake is van een duidelijke uitzondering op grond van de wet.

Daarbij geldt:

- voor leerlingen jonger dan 16 jaar wordt toestemming gevraagd aan ouders/verzorgers;
- leerlingen van 16 jaar en ouder geven zelf toestemming;
- toestemming wordt bij voorkeur per gebruiksdoel of kanaal gevraagd;
- intrekking van toestemming wordt zo spoedig mogelijk verwerkt.

Toestemming voor beeldmateriaal wordt afzonderlijk gevraagd en niet opgenomen als verborgen onderdeel van een algemeen formulier.

4.7 Bijzondere persoonsgegevens

Bijzondere persoonsgegevens, zoals gegevens over gezondheid, worden alleen verwerkt indien daarvoor een specifieke wettelijke grondslag of uitzondering bestaat. De verwerking van deze gegevens vindt plaats met extra zorgvuldigheid en wordt beperkt tot hetgeen strikt noodzakelijk is.

Toegang tot dergelijke gegevens wordt alleen verleend aan personen die deze informatie nodig hebben voor de uitvoering van hun taak.

4.8 Vastlegging

Van iedere structurele verwerking wordt vastgelegd op welke rechtsgrond deze berust. Dit gebeurt in ieder geval in het verwerkingsregister en, waar nodig, in aanvullende procedures of documentatie.

Wanneer een verwerking wijzigt, wordt opnieuw beoordeeld of de gekozen rechtsgrond nog passend is.

5. Verwerkingsregister

5.1 Algemeen

De schoolorganisatie houdt een actueel verwerkingsregister bij. Hiermee wordt inzichtelijk gemaakt welke persoonsgegevens worden verwerkt, voor welke doeleinden dit gebeurt en op welke wijze de verwerking is ingericht en beveiligd.

Het verwerkingsregister is een belangrijk onderdeel van de verantwoordingsplicht en ondersteunt de organisatie bij het aantoonbaar naleven van de AVG.

5.2 Doel van het verwerkingsregister

Het verwerkingsregister heeft tot doel:

- inzicht te geven in alle structurele verwerkingen van persoonsgegevens;
- vast te leggen op welke rechtsgrond een verwerking berust;
- duidelijk te maken welke gegevens worden verwerkt en met wie deze worden gedeeld;
- bewaartermijnen en beveiligingsmaatregelen te documenteren;
- risico's en aandachtspunten tijdig te signaleren;
- ondersteuning te bieden bij audits, controles, rechtenverzoeken en incidenten.

5.3 Inhoud van het verwerkingsregister

In het verwerkingsregister worden van iedere relevante verwerking ten minste de volgende onderdelen vastgelegd:

- naam of omschrijving van de verwerking;
- doel van de verwerking;
- categorieën van betrokkenen;
- categorieën van persoonsgegevens;
- rechtsgrond van de verwerking;
- ontvangers of categorieën van ontvangers;
- eventuele verwerkers en subverwerkers;

- bewaartermijn of criteria voor het bepalen daarvan;
- algemene beschrijving van de beveiligingsmaatregelen;
- verantwoordelijke proceseigenaar of contactpersoon.

Waar van toepassing worden ook doorgiften aan derden, koppelingen met systemen en een verwijzing naar aanvullende documentatie opgenomen.

5.4 Reikwijdte van het register

Het verwerkingsregister omvat in ieder geval de structurele verwerkingen van persoonsgegevens binnen de schoolorganisatie, zoals verwerkingen in het kader van:

- leerlingadministratie;
- personeelsadministratie;
- onderwijs en begeleiding;
- communicatie met ouders/verzorgers;
- digitale leermiddelen en onderwijssystemen;
- ICT-beheer en informatiebeveiliging;
- sollicitatieprocedures;
- samenwerking met externe partijen en leveranciers.

Ook verwerkingen die door externe partijen in opdracht van de school worden uitgevoerd, worden opgenomen voor zover de school daarvoor verantwoordelijk is.

5.5 Beheer en actualisatie

Het verwerkingsregister wordt centraal beheerd en periodiek gecontroleerd op actualiteit en volledigheid. Nieuwe verwerkingen, wijzigingen in bestaande processen en beëindiging van verwerkingen worden tijdig verwerkt in het register.

Actualisatie van het register vindt in ieder geval plaats bij:

- invoering van nieuwe systemen, applicaties of processen;
- wijzigingen in doelen, gegevenscategorieën of rechtsgrondslagen;
- inzet van nieuwe verwerkers of leveranciers;
- wijzigingen in bewaartermijnen of beveiligingsmaatregelen;

- organisatorische veranderingen die gevolgen hebben voor gegevensverwerking.

5.6 Verantwoordelijkheid

Het bevoegd gezag is eindverantwoordelijk voor het bijhouden van een actueel en volledig verwerkingsregister. De feitelijke uitvoering kan worden belegd bij een privacycoördinator, IBP-coördinator of andere aangewezen functionaris.

Proceseigenaren, schoolleiding, ICT en andere betrokken functionarissen leveren de informatie aan die nodig is om het register juist en actueel te houden.

5.7 Gebruik en controle

Het verwerkingsregister wordt gebruikt als intern sturings- en controlemiddel. Het ondersteunt de organisatie bij:

- het beoordelen van rechtmatigheid en noodzaak van verwerkingen;
- het beantwoorden van vragen van betrokkenen;
- het afhandelen van datalekken en incidenten;
- het opstellen van verwerkersovereenkomsten;
- het uitvoeren van risicoanalyses of DPIA's;
- het voorbereiden van interne of externe controles.

Het register wordt periodiek beoordeeld op volledigheid, juistheid en samenhang met het feitelijke gebruik van persoonsgegevens binnen de organisatie.

6. Leveranciers en digitale leermiddelen

6.1 Algemeen

Bij de inzet van leveranciers en digitale leermiddelen verwerkt de school uitsluitend persoonsgegevens wanneer dit noodzakelijk, rechtmatig en zorgvuldig gebeurt. Hierbij wordt steeds beoordeeld welke gegevens worden verwerkt, voor welk doel dit gebeurt en welke verantwoordelijkheden daarbij gelden.

De school blijft verantwoordelijk voor een zorgvuldige omgang met persoonsgegevens wanneer verwerkingen plaatsvinden met behulp van externe partijen of digitale toepassingen.

6.2 Verwerkers en verwerkersovereenkomst

Wanneer een leverancier in opdracht van de school persoonsgegevens verwerkt, wordt deze leverancier aangemerkt als verwerker. In dat geval worden schriftelijke afspraken gemaakt in een verwerkersovereenkomst.

In een verwerkersovereenkomst worden in ieder geval afspraken vastgelegd over:

- het doel en de duur van de verwerking;
- de aard van de persoonsgegevens en de categorieën betrokkenen;
- de geheimhoudingsplicht;
- passende technische en organisatorische beveiligingsmaatregelen;
- de inzet van eventuele subverwerkers;
- de meldplicht bij datalekken en beveiligingsincidenten;
- de verwijdering of teruggave van gegevens na afloop van de dienstverlening;
- de mogelijkheid tot controle op naleving van de afspraken.

6.3 Selectie en beoordeling van leveranciers

Voordat een leverancier of digitale toepassing in gebruik wordt genomen, beoordeelt de school of het gebruik daarvan verenigbaar is met de AVG en met het eigen privacy- en informatiebeveiligingsbeleid.

Daarbij wordt in ieder geval gekeken naar:

- het doel van de verwerking;
- de noodzaak van het gebruik van het product of de dienst;
- welke persoonsgegevens worden verwerkt;
- of de leverancier optreedt als verwerker of als zelfstandig verwerkingsverantwoordelijke;
- de beveiligingsmaatregelen van de leverancier;
- de locatie van gegevensopslag;
- de inzet van subverwerkers;
- de mogelijkheden voor beheer, verwijdering en beëindiging van de dienstverlening.

6.4 Digitale leermiddelen

Bij het gebruik van digitale leermiddelen wordt terughoudend en zorgvuldig omgegaan met persoonsgegevens van leerlingen. Alleen digitale leermiddelen die passend zijn binnen de onderwijsdoelen en voldoen aan de privacy- en beveiligingseisen van de school worden ingezet.

De school beoordeelt bij digitale leermiddelen onder meer:

- welke persoonsgegevens noodzakelijk zijn voor gebruik;
- of kan worden gewerkt met zo min mogelijk identificerende gegevens;
- of instellingen privacyvriendelijk kunnen worden ingericht;
- of gegevens niet voor eigen commerciële of andere niet-noodzakelijke doeleinden worden gebruikt;
- of passende afspraken met de leverancier zijn gemaakt.

6.5 Gebruik door medewerkers

Medewerkers maken uitsluitend gebruik van door de school goedgekeurde leveranciers, applicaties en digitale leermiddelen voor zover daarbij persoonsgegevens worden verwerkt. Het is niet toegestaan om op eigen initiatief applicaties of online diensten te gebruiken waarin persoonsgegevens van leerlingen, ouders/verzorgers of medewerkers worden verwerkt, zonder voorafgaande beoordeling en toestemming.

Hiermee wordt voorkomen dat persoonsgegevens worden verwerkt via niet-getoetste of onvoldoende beveiligde middelen.

6.6 Delen van gegevens met leveranciers

Persoonsgegevens worden alleen gedeeld met leveranciers indien dit noodzakelijk is voor de uitvoering van de dienstverlening en indien daarvoor een geldige grondslag bestaat. De school deelt niet meer gegevens dan nodig is en beoordeelt vooraf of de verstrekking passend en proportioneel is.

Indien mogelijk wordt gewerkt met beperkte datasets, afgeschermde gegevens of pseudonimisering.

6.7 Beëindiging van dienstverlening

Bij beëindiging van een overeenkomst met een leverancier wordt geborgd dat persoonsgegevens op een zorgvuldige wijze worden verwijderd, teruggegeven of overgedragen, afhankelijk van de aard van de dienstverlening en de gemaakte afspraken.

De school ziet erop toe dat:

- toegang tot systemen tijdig wordt beëindigd;
- gegevens niet langer beschikbaar blijven dan noodzakelijk;
- gemaakte afspraken over verwijdering of retournering worden nageleefd;
- het verwerkingsregister en de bijbehorende documentatie waar nodig worden bijgewerkt.

6.8 Verantwoordelijkheid

Het bevoegd gezag is eindverantwoordelijk voor de zorgvuldige selectie, contractering en aansturing van leveranciers die persoonsgegevens verwerken. De uitvoering hiervan kan binnen de organisatie worden ondersteund door schoolleiding, ICT, privacycoördinatie of andere aangewezen functionarissen.

Iedere medewerker draagt verantwoordelijkheid voor het naleven van de interne afspraken over het gebruik van leveranciers en digitale leermiddelen.

7. Leerlingdossier en inzage

7.1 Algemeen

De school legt van iedere leerling een dossier aan voor zover dit noodzakelijk is voor het verzorgen van onderwijs, de begeleiding van de leerling en het uitvoeren van wettelijke taken. Het leerlingdossier wordt zorgvuldig samengesteld en beheerd.

7.2 Doel van het leerlingdossier

Het leerlingdossier heeft tot doel om relevante informatie vast te leggen die nodig is voor:

- de onderwijsontwikkeling van de leerling;
- begeleiding en ondersteuning;
- voortgang en resultaten;
- aanwezigheid en verzuim;
- communicatie met ouders/verzorgers;
- het voldoen aan wettelijke verplichtingen.

Alleen gegevens die voor deze doeleinden noodzakelijk zijn, worden opgenomen in het dossier.

7.3 Inhoud van het leerlingdossier

Het leerlingdossier kan, voor zover relevant, bestaan uit:

- identificatie- en contactgegevens;
- administratieve gegevens;
- gegevens over inschrijving, aanwezigheid en schoolloopbaan;
- toetsresultaten en voortgangsgegevens;
- verslagen over begeleiding en ondersteuning;
- relevante correspondentie en afspraken met ouders/verzorgers;
- andere gegevens die noodzakelijk zijn voor onderwijs en begeleiding.

De school neemt geen gegevens op die niet relevant, bovenmatig of onnodig belastend zijn.

7.4 Zorgvuldige dossiervorming

Gegevens in het leerlingdossier worden zorgvuldig, feitelijk en terughoudend vastgelegd. Medewerkers zorgen ervoor dat informatie in het dossier:

- relevant is voor het doel van de verwerking;
- juist en zo nodig actueel is;
- zakelijk en professioneel is geformuleerd;
- herleidbaar is tot de medewerker of bron die de informatie heeft vastgelegd, indien van toepassing.

Persoonlijke meningen, vermoedens of niet-noodzakelijke kwalificaties worden niet opgenomen, tenzij deze functioneel en voldoende onderbouwd zijn in het kader van de begeleiding of ondersteuning van de leerling.

7.5 Toegang tot het leerlingdossier

Toegang tot het leerlingdossier is beperkt tot medewerkers die deze gegevens nodig hebben voor de uitvoering van hun werkzaamheden. De toegang wordt verleend op basis van functie, rol en taak.

De school draagt er zorg voor dat:

- alleen bevoegde personen inzage hebben;
- autorisaties zorgvuldig worden toegekend en beheerd;
- gegevens niet worden ingezien zonder functionele noodzaak;
- vertrouwelijkheid van dossierinformatie wordt gewaarborgd.

7.6 Inzage door ouders, verzorgers en leerlingen

Ouders/verzorgers en, voor zover van toepassing, leerlingen hebben recht op inzage in de persoonsgegevens die door de school over hen of over de leerling worden verwerkt, voor zover de wet daaraan niet in de weg staat.

Verzoeken om inzage worden behandeld volgens de geldende procedure voor rechten van betrokkenen. Daarbij wordt beoordeeld:

- wie het verzoek doet;
- of de identiteit voldoende is vastgesteld;
- op welke gegevens het verzoek betrekking heeft;
- of er wettelijke beperkingen of uitzonderingen van toepassing zijn.

7.7 Inzage door derden

Gegevens uit het leerlingdossier worden niet verstrekt aan derden, tenzij daarvoor een wettelijke verplichting bestaat, de verstrekking noodzakelijk is voor de uitvoering van de onderwijstaak, of een andere geldige grondslag van toepassing is.

Indien gegevens met derden worden gedeeld, gebeurt dit zorgvuldig en beperkt tot wat noodzakelijk is.

7.8 Inzage door toezichthoudende instanties

Indien een bevoegde toezichthoudende instantie, zoals de Inspectie van het Onderwijs, op grond van een wettelijke taak inzage nodig heeft in leerlinggegevens, verleent de school hieraan medewerking voor zover dit rechtmatig en noodzakelijk is.

De school beperkt de inzage of verstrekking daarbij tot de gegevens die voor dat doel noodzakelijk zijn.

7.9 Bewaren en verwijderen

Gegevens in het leerlingdossier worden niet langer bewaard dan noodzakelijk is voor het doel waarvoor zij zijn verwerkt, tenzij een wettelijke bewaartermijn van toepassing is. De school legt bewaartermijnen vast in het verwerkingsregister en, waar nodig, in een afzonderlijke bewaartermijnenmatrix.

7.10 Verantwoordelijkheid

De schoolleiding ziet toe op een zorgvuldige omgang met leerlingdossiers binnen de school. Medewerkers zijn verantwoordelijk voor een correcte, terughoudende en professionele vastlegging van gegevens in het dossier.

8. Rechten van betrokkenen

8.1 Algemeen

De school respecteert de rechten van betrokkenen met betrekking tot de verwerking van persoonsgegevens. Betrokkenen kunnen de school verzoeken om informatie over de verwerking van hun persoonsgegevens en, voor zover de wet daarin voorziet, gebruikmaken van hun privacyrechten.

8.2 Welke rechten betrokkenen hebben

Betrokkenen kunnen, afhankelijk van de situatie, een beroep doen op de volgende rechten:

- recht op informatie;
- recht op inzage;
- recht op rectificatie;
- recht op wissing;
- recht op beperking van de verwerking;
- recht van bezwaar;
- recht op overdraagbaarheid van gegevens, voor zover van toepassing.

De school beoordeelt per verzoek in hoeverre het betreffende recht van toepassing is.

8.3 Indienen van een verzoek

Een verzoek tot uitoefening van een privacyrecht wordt ingediend via het door de school aangewezen contactpunt, bijvoorbeeld een centraal e-mailadres of formulier. In het verzoek wordt zo duidelijk mogelijk aangegeven op welke persoonsgegevens of verwerking het verzoek betrekking heeft.

De school kan, indien nodig, aanvullende informatie vragen om het verzoek zorgvuldig te kunnen behandelen.

8.4 Identiteitscontrole

Voordat een verzoek inhoudelijk wordt behandeld, beoordeelt de school of de identiteit van de verzoeker voldoende vaststaat. Indien nodig vraagt de school om aanvullende verificatie.

De school vraagt daarbij niet meer gegevens op dan noodzakelijk is voor een zorgvuldige controle van de identiteit.

8.5 Behandeling van verzoeken

Verzoeken van betrokkenen worden zorgvuldig, vertrouwelijk en binnen de geldende wettelijke termijn behandeld. De school beoordeelt:

- of het verzoek duidelijk is;
- of de verzoeker gerechtigd is om het verzoek te doen;
- op welke persoonsgegevens het verzoek betrekking heeft;
- of wettelijke uitzonderingen of beperkingen van toepassing zijn.

Indien nodig worden bij de behandeling van het verzoek de schoolleiding, privacycoördinator, ICT of andere betrokken functionarissen geraadpleegd.

8.6 Termijnen

De school handelt verzoeken van betrokkenen tijdig af en binnen de daarvoor geldende wettelijke termijn. Indien een verzoek complex is of wanneer sprake is van meerdere verzoeken, kan de afhandeling worden verlengd voor zover de wet dit toestaat.

Indien een verlenging nodig is, wordt de verzoeker hierover tijdig geïnformeerd.

8.7 Afwijzing of beperking van een verzoek

Indien een verzoek geheel of gedeeltelijk niet kan worden uitgevoerd, motiveert de school dit op duidelijke wijze. Daarbij wordt aangegeven waarom het verzoek wordt afgewezen of beperkt en, voor zover van toepassing, op welke wettelijke grond dit berust.

8.8 Vastlegging

De school legt ontvangen verzoeken en de afhandeling daarvan vast in een daarvoor bestemd overzicht of register. Daarbij wordt in ieder geval vastgelegd:

- datum van ontvangst;
- aard van het verzoek;
- datum van afhandeling;
- uitkomst van het verzoek;
- eventuele bijzonderheden of motivering.

8.9 Verantwoordelijkheid

Het bevoegd gezag is eindverantwoordelijk voor de zorgvuldige afhandeling van verzoeken van betrokkenen. De feitelijke behandeling kan worden belegd bij de schoolleiding, privacycoördinator of andere aangewezen functionaris.

Medewerkers die betrokken zijn bij de uitvoering van een verzoek werken mee aan een juiste en tijdige afhandeling.

9. Bewaartermijnen

9.1 Algemeen

De school bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor deze zijn verzameld of verwerkt, tenzij een wettelijke bewaarplicht of andere geldige grond een langere bewaartermijn vereist.

9.2 Uitgangspunt

Voor alle verwerkingen van persoonsgegevens geldt dat de bewaartermijn wordt afgestemd op:

- het doel van de verwerking;
- de toepasselijke wet- en regelgeving;
- administratieve en organisatorische noodzaak;
- de belangen van betrokkenen.

Zodra persoonsgegevens niet langer nodig zijn, worden deze verwijderd, vernietigd of geanonimiseerd, voor zover de wet of het belang van de organisatie zich daar niet tegen verzet.

9.3 Vastlegging van bewaartermijnen

De school legt bewaartermijnen vast in het verwerkingsregister en, waar nodig, in een afzonderlijke bewaartermijnenmatrix. Per gegevenscategorie of verwerkingsproces wordt daarbij vastgesteld:

- welke gegevens worden bewaard;
- voor welk doel;
- welke bewaartermijn geldt;
- op welk moment de bewaartermijn ingaat;
- op welke wijze gegevens na afloop worden verwijderd of vernietigd.

9.4 Toepassing in de praktijk

Bewaartermijnen gelden voor zowel digitale als papieren gegevensdragers. Dit omvat onder meer:

- leerlingdossiers;
- personeelsdossiers;
- toets- en voortgangsgegevens;
- e-mailberichten;
- camerabeelden;

- sollicitatiegegevens;
- logbestanden;
- administratieve documenten.

Ook persoonsgegevens in netwerkschijven, mailboxen, lokale opslag en back-ups vallen onder het bewaarbeleid, voor zover daarop persoonsgegevens zijn opgeslagen.

9.5 Periodieke controle en opschoning

De school voert periodiek controles uit op de naleving van bewaartermijnen. Gegevens die niet langer bewaard mogen worden, worden tijdig verwijderd of vernietigd.

Waar mogelijk worden systemen en processen zodanig ingericht dat opschoning structureel en beheersbaar plaatsvindt.

9.6 Uitzonderingen

Indien persoonsgegevens langer moeten worden bewaard vanwege:

- een wettelijke verplichting;
- een lopende procedure, klacht of geschil;
- een verzoek van een toezichthouder;
- een zwaarwegend organisatorisch belang,

dan wordt dit gemotiveerd vastgelegd. In dat geval worden de betreffende gegevens alleen langer bewaard voor zover dat noodzakelijk is.

9.7 Verantwoordelijkheid

Het bevoegd gezag is eindverantwoordelijk voor het vaststellen en naleven van bewaartermijnen. De praktische uitvoering kan worden belegd bij de schoolleiding, administratie, privacycoördinator, ICT of andere aangewezen functionarissen.

Medewerkers zijn verantwoordelijk voor een zorgvuldige omgang met persoonsgegevens binnen de systemen en dossiers waarmee zij werken, en voor het naleven van de geldende bewaartermijnen en verwijderprocedures.

10. Informatiebeveiliging (IBP)

10.1 Algemeen

De school treft passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies, onbevoegde toegang, onrechtmatige verwerking en andere vormen van misbruik.

Informatiebeveiliging is een vast onderdeel van de organisatie en ondersteunt een zorgvuldige, betrouwbare en continue verwerking van persoonsgegevens.

10.2 Doel

Het informatiebeveiligingsbeleid heeft tot doel:

- persoonsgegevens en andere vertrouwelijke informatie te beschermen;
- risico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te beperken;
- de continuïteit van onderwijs en bedrijfsvoering te ondersteunen;
- te voldoen aan wettelijke verplichtingen en interne beleidskaders.

10.3 Uitgangspunten

Bij informatiebeveiliging hanteert de school in ieder geval de volgende uitgangspunten:

- toegang tot systemen en gegevens is beperkt tot bevoegde personen;
- beveiligingsmaatregelen zijn passend bij de aard van de gegevens en de risico's;
- systemen en apparaten worden zorgvuldig beheerd en onderhouden;
- medewerkers gaan veilig om met gegevens, accounts en apparatuur;
- beveiligingsincidenten worden tijdig gesignaleerd en opgevolgd.

10.4 Toegangsbeveiliging

De school zorgt voor passende maatregelen rondom toegang tot systemen en gegevens. Dit houdt onder meer in dat:

- accounts persoonlijk en niet overdraagbaar zijn;

- wachtwoorden zorgvuldig worden beheerd;
- waar mogelijk aanvullende beveiliging, zoals meerfactorauthenticatie, wordt toegepast;
- autorisaties worden toegekend op basis van functie en taak;
- autorisaties tijdig worden aangepast of ingetrokken bij functiewijziging of uitdiensttreding.

10.5 Beveiliging van systemen en apparaten

Systemen, netwerken en apparaten worden passend beveiligd en beheerd. Dit omvat onder meer:

- tijdige installatie van updates en beveiligingspatches;
- gebruik van antivirus- of andere beveiligingssoftware waar nodig;
- beveiliging van laptops, tablets en andere apparaten;
- versleuteling of andere passende maatregelen bij opslag en transport van gegevens;
- regelmatige back-up van belangrijke gegevens en systemen.

10.6 Veilige opslag en verzending

Persoonsgegevens worden zorgvuldig opgeslagen en verzonden. Daarbij geldt dat:

- gebruik wordt gemaakt van goedgekeurde systemen en opslaglocaties;
- persoonsgegevens alleen via passende en beveiligde middelen worden gedeeld;
- terughoudend wordt omgegaan met het verzenden van privacygevoelige informatie;
- gegevensdragers en documenten met persoonsgegevens niet onbeheerd worden achtergelaten.

10.7 Werken op afstand en gebruik van apparatuur

Bij thuiswerken of werken op afstand blijven de beveiligingsregels onverkort van toepassing. Medewerkers dragen er zorg voor dat persoonsgegevens ook buiten de schoolomgeving zorgvuldig worden verwerkt.

Indien gebruik wordt gemaakt van mobiele apparatuur of andere werkmiddelen, gebeurt dit volgens de geldende afspraken over beveiliging, toegang en opslag.

10.8 Incidenten en beveiligingsrisico's

Beveiligingsincidenten en signalen van misbruik, verlies of onbevoegde toegang worden direct gemeld volgens de interne procedure. De school beoordeelt incidenten zorgvuldig en treft waar nodig maatregelen om schade te beperken en herhaling te voorkomen.

Indien sprake is van een datalek, wordt gehandeld volgens het datalekprotocol.

10.9 Bewustwording en naleving

Informatiebeveiliging is niet alleen een technische aangelegenheid, maar ook een verantwoordelijkheid van alle medewerkers. De school bevordert daarom bewustwording en zorgvuldig gedrag door middel van instructie, ondersteuning en periodieke aandacht voor veilig werken.

Van medewerkers wordt verwacht dat zij de geldende beveiligingsmaatregelen naleven en onveilige situaties tijdig signaleren.

10.10 Verantwoordelijkheid

Het bevoegd gezag is eindverantwoordelijk voor het informatiebeveiligingsbeleid. De uitvoering en bewaking hiervan worden binnen de organisatie belegd bij de schoolleiding, ICT, privacycoördinatie en andere aangewezen functionarissen.

Iedere medewerker is binnen de eigen werkzaamheden verantwoordelijk voor een veilige en zorgvuldige omgang met persoonsgegevens en informatiesystemen.

11. Datalekken en incidenten

11.1 Algemeen

De school handelt zorgvuldig bij beveiligingsincidenten en datalekken. Een datalek is een inbreuk op de beveiliging die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van, dan wel ongeoorloofde toegang tot persoonsgegevens.

11.2 Meldplicht binnen de organisatie

Iedere medewerker die kennisneemt van een (mogelijk) datalek of beveiligingsincident meldt dit direct via de interne meldprocedure. Tijdige melding is noodzakelijk om risico's te beperken en passende maatregelen te kunnen treffen.

11.3 Eerste maatregelen

Na een melding worden zo spoedig mogelijk maatregelen getroffen om het incident te beperken en verdere schade te voorkomen. Afhankelijk van de situatie kan dit onder meer bestaan uit:

- het blokkeren van accounts of toegang;
- het intrekken van verzonden links of gedeelde documenten;
- het veiligstellen van systemen of apparaten;
- het herstellen van onjuiste instellingen;
- het beperken van verdere verspreiding van gegevens.

11.4 Beoordeling van het incident

De school beoordeelt ieder incident zorgvuldig. Daarbij wordt in ieder geval gekeken naar:

- de aard van het incident;
- welke persoonsgegevens betrokken zijn;
- hoeveel personen mogelijk zijn getroffen;
- de mogelijke gevolgen voor betrokkenen;

- de kans op misbruik of schade;
- de maatregelen die al zijn genomen.

11.5 Registratie

Alle datalekken en relevante beveiligingsincidenten worden vastgelegd in een datalekregister of ander daarvoor bestemd overzicht. Ook incidenten die niet leiden tot een melding aan de toezichthouder worden geregistreerd, zodat de school inzicht houdt in aard, omvang en opvolging.

11.6 Melding aan de Autoriteit Persoonsgegevens

Indien een datalek waarschijnlijk een risico oplevert voor de rechten en vrijheden van betrokkenen, beoordeelt de school of melding aan de Autoriteit Persoonsgegevens noodzakelijk is. Deze beoordeling vindt zo spoedig mogelijk plaats.

11.7 Informeren van betrokkenen

Wanneer een datalek waarschijnlijk een hoog risico oplevert voor de betrokkenen, worden zij hierover geïnformeerd, tenzij een wettelijke uitzondering van toepassing is. De communicatie aan betrokkenen is duidelijk en bevat in ieder geval informatie over de aard van het incident en de mogelijke gevolgen.

11.8 Opvolging en evaluatie

Na afloop van een incident beoordeelt de school of aanvullende maatregelen nodig zijn om herhaling te voorkomen. Waar nodig worden processen, systemen, instructies of beveiligingsmaatregelen aangepast.

11.9 Verantwoordelijkheid

Het bevoegd gezag is eindverantwoordelijk voor de zorgvuldige afhandeling van datalekken en beveiligingsincidenten. De praktische coördinatie kan worden belegd bij de schoolleiding, privacycoördinator, ICT of andere aangewezen functionarissen.

Iedere medewerker is verantwoordelijk voor het tijdig signaleren en melden van mogelijke datalekken en incidenten.

12. DPIA (Data Protection Impact Assessment)

12.1 Algemeen

Wanneer een verwerking van persoonsgegevens waarschijnlijk een hoog privacyrisico met zich meebrengt, voert de school vooraf een gegevensbeschermingseffectbeoordeling (DPIA) uit. Een DPIA helpt om privacyrisico's tijdig in beeld te brengen en passende maatregelen te treffen voordat de verwerking start of wijzigt.

12.2 Doel

Het doel van een DPIA is:

- het in kaart brengen van privacyrisico's;
- het beoordelen van de noodzaak en proportionaliteit van een verwerking;
- het bepalen van passende maatregelen om risico's te beperken;
- het onderbouwen van een zorgvuldige en aantoonbare besluitvorming.

12.3 Wanneer een DPIA wordt uitgevoerd

De school beoordeelt vooraf of een DPIA nodig is, in het bijzonder bij verwerkingen die kunnen leiden tot een verhoogd risico voor betrokkenen. Dit kan onder meer aan de orde zijn bij:

- grootschalige of systematische monitoring;
- nieuwe systemen of toepassingen waarin veel persoonsgegevens worden verwerkt;
- nieuwe koppelingen tussen systemen;
- structurele verwerking van bijzondere persoonsgegevens;
- inzet van biometrie of cameratoezicht;
- gebruik van nieuwe technologieën, zoals AI-toepassingen;
- verwerkingen die op andere wijze een verhoogd risico voor leerlingen, ouders/verzorgers of medewerkers meebrengen.

12.4 Inhoud van een DPIA

In een DPIA wordt in ieder geval aandacht besteed aan:

- het doel en de aard van de verwerking;
- de categorieën persoonsgegevens en betrokkenen;
- de noodzaak en proportionaliteit van de verwerking;
- de privacyrisico's voor betrokkenen;
- de maatregelen om deze risico's te beperken;
- de resterende risico's en de afweging daarover.

12.5 Procedure

Een DPIA wordt uitgevoerd voordat een risicovolle verwerking start of wezenlijk wordt gewijzigd. Bij de uitvoering worden, waar nodig, de relevante functionarissen betrokken, zoals schoolleiding, privacycoördinatie, ICT en de Functionaris voor Gegevensbescherming.

De uitkomsten van de DPIA worden vastgelegd. Indien uit de beoordeling blijkt dat aanvullende maatregelen nodig zijn, worden deze meegenomen in de inrichting van de verwerking.

12.6 Verantwoordelijkheid

Het bevoegd gezag is eindverantwoordelijk voor het tijdig uitvoeren van een DPIA wanneer dit nodig is. De praktische uitvoering kan worden belegd bij de privacycoördinator, schoolleiding of andere aangewezen functionaris, in afstemming met ICT en de Functionaris voor Gegevensbescherming.

12.7 Vastlegging en herbeoordeling

De school legt vast wanneer een DPIA is uitgevoerd, wat de uitkomsten zijn en welke maatregelen zijn getroffen. Indien een verwerking later wijzigt of nieuwe risico's ontstaan, wordt beoordeeld of een herbeoordeling nodig is.

13. Beeldmateriaalbeleid

13.1 Algemeen

De school gaat zorgvuldig om met foto's, video's en ander beeldmateriaal waarop leerlingen, medewerkers of andere betrokkenen herkenbaar in beeld zijn. Bij het maken, gebruiken en publiceren van beeldmateriaal wordt rekening gehouden met privacy, veiligheid en de geldende wettelijke regels.

13.2 Doel

Beeldmateriaal wordt alleen gemaakt en gebruikt voor duidelijke en gerechtvaardigde doeleinden, zoals:

- communicatie over schoolactiviteiten;
- informatievoorziening aan ouders/verzorgers;
- gebruik binnen de schoolorganisatie;
- verslaglegging of promotie van schoolactiviteiten, voor zover passend.

De school maakt of gebruikt geen beeldmateriaal voor andere doeleinden zonder dat hiervoor een geldige grondslag bestaat.

13.3 Toestemming

Wanneer voor het maken of publiceren van herkenbaar beeldmateriaal toestemming vereist is, wordt deze vooraf gevraagd. Toestemming wordt afzonderlijk en duidelijk vastgelegd.

Daarbij geldt dat:

- voor leerlingen jonger dan 16 jaar toestemming wordt gevraagd aan ouders/verzorgers;
- leerlingen van 16 jaar en ouder zelf toestemming geven;
- toestemming specifiek wordt gevraagd per doel of kanaal, voor zover dat nodig is;
- toestemming altijd kan worden ingetrokken.

13.4 Gebruik en publicatie

De school publiceert beeldmateriaal alleen voor zover dit past binnen het doel waarvoor toestemming is gegeven of een andere geldige grondslag bestaat. Bij publicatie wordt terughoudend omgegaan met de combinatie van beeldmateriaal en persoonsgegevens, zoals volledige namen.

De school beoordeelt steeds of publicatie noodzakelijk en passend is.

13.5 Intrekking van toestemming

Indien toestemming voor het gebruik van beeldmateriaal wordt ingetrokken, verwerkt de school dit zo spoedig mogelijk. Vanaf dat moment wordt het betreffende beeldmateriaal niet opnieuw gebruikt of gepubliceerd, voor zover dit redelijkerwijs mogelijk is.

13.6 Interne werkwijze

De school draagt er zorg voor dat medewerkers op de hoogte zijn van de afspraken rondom beeldmateriaal. Bij het maken, opslaan en delen van foto's en video's wordt zorgvuldig gehandeld en worden alleen goedgekeurde middelen en kanalen gebruikt.

13.7 Verantwoordelijkheid

Het bevoegd gezag is eindverantwoordelijk voor een zorgvuldige omgang met beeldmateriaal. De schoolleiding ziet toe op naleving binnen de school. Medewerkers zijn verantwoordelijk voor een zorgvuldige toepassing van de geldende afspraken bij het maken en gebruiken van beeldmateriaal.

14. Communicatie en training

14.1 Algemeen

De school vindt het belangrijk dat medewerkers zorgvuldig omgaan met persoonsgegevens en zich bewust zijn van hun verantwoordelijkheden op het gebied van privacy en informatiebeveiliging. Duidelijke communicatie en regelmatige training dragen bij aan een veilige en zorgvuldige werkwijze binnen de organisatie.

14.2 Doel

Communicatie en training zijn erop gericht om:

- kennis van privacyregels en informatiebeveiliging te vergroten;
- bewustwording te bevorderen bij medewerkers;
- zorgvuldig handelen in de praktijk te ondersteunen;
- risico's op fouten, datalekken en onbevoegde toegang te beperken;
- een gezamenlijke verantwoordelijkheid binnen de organisatie te versterken.

14.3 Instructie aan medewerkers

Medewerkers ontvangen periodiek voorlichting en instructie over privacy en informatiebeveiliging. Daarbij wordt in ieder geval aandacht besteed aan:

- zorgvuldig omgaan met persoonsgegevens;
- veilig gebruik van systemen en accounts;
- het herkennen en melden van datalekken en incidenten;
- vertrouwelijkheid en need-to-know;
- veilig communiceren en delen van gegevens;
- praktische afspraken binnen de school.

14.4 Nieuwe medewerkers, stagiairs en vrijwilligers

Nieuwe medewerkers, stagiairs en vrijwilligers worden bij de start van hun werkzaamheden geïnformeerd over de geldende privacy- en beveiligingsregels. Voor zover relevant ontvangen zij uitleg over hun verantwoordelijkheden, de interne procedures en het gebruik van systemen.

14.5 Periodieke aandacht en actualisatie

De school besteedt periodiek aandacht aan privacy en informatiebeveiliging, bijvoorbeeld via teamoverleggen, instructiemomenten, interne communicatie of gerichte bewustwordingsactiviteiten. Indien wetgeving, beleid of werkwijzen wijzigen, wordt de communicatie en training daarop aangepast.

14.6 Verantwoordelijkheid

Het bevoegd gezag is eindverantwoordelijk voor het bevorderen van bewustwording en kennis op het gebied van privacy en informatiebeveiliging. De schoolleiding draagt zorg voor de praktische uitvoering binnen de school. Medewerkers zijn verantwoordelijk voor het toepassen van de gegeven instructies in hun dagelijkse werkzaamheden.

15. Documenten en bijlagen

15.1 Algemeen

Bij dit privacybeleid horen aanvullende documenten en bijlagen die de praktische uitvoering van het beleid ondersteunen. Deze documenten bevatten nadere uitwerkingen, procedures, contactgegevens en formats die binnen de organisatie worden gebruikt.

15.2 Doel

De documenten en bijlagen hebben tot doel om:

- het privacybeleid praktisch toepasbaar te maken;
- medewerkers te ondersteunen bij een zorgvuldige uitvoering;
- verantwoordelijkheden, werkwijzen en contactpunten vast te leggen;
- te zorgen voor eenduidige documentatie binnen de organisatie.

15.3 Bijbehorende documenten

Bij dit beleid kunnen onder meer de volgende documenten en bijlagen behoren:

- contactgegevens van betrokken functionarissen;
- privacyverklaringen;
- het verwerkingsregister;
- de bewaartermijnenmatrix;
- het datalekprotocol en meldformulier;
- formats voor rechtenverzoeken;
- toestemmingsformulieren, waaronder voor beeldmateriaal;
- verwerkersovereenkomsten en controlelijsten voor leveranciers;
- aanvullende interne procedures op het gebied van privacy en informatiebeveiliging.

15.4 Beheer en actualisatie

De bij dit beleid behorende documenten worden beheerd en waar nodig geactualiseerd. Wanneer wetgeving, processen, systemen of contactgegevens wijzigen, worden ook de bijlagen en ondersteunende documenten aangepast.

15.5 Toegankelijkheid

De relevante documenten en bijlagen zijn beschikbaar voor de medewerkers en functionarissen die deze nodig hebben voor de uitvoering van hun werkzaamheden. Voor zover van toepassing worden ook betrokkenen geïnformeerd over documenten die voor hen van belang zijn, zoals privacyverklaringen en toestemmingsformulieren.

15.6 Verantwoordelijkheid

Het bevoegd gezag is eindverantwoordelijk voor de vaststelling van het beleid en de daarbij behorende documenten. De praktische uitwerking, het beheer en de actualisatie kunnen worden belegd bij de schoolleiding, privacycoördinator of andere aangewezen functionarissen.