Intern Privacybeleid

DELTA-ONDERWIJS

ICTRecht Privacy B.V.
Jollemanhof 12
1019 GW Amsterdam

TELEFOON
020 663 1941

E-MAIL
privacy@ictrecht.nl

INTERNET
ictrecht.nl/privacy

KVK
72602651

BTW
NL859169820B01

IBAN
NL64 RABO 0334 0962 94

Versie	Datum	Status	Door
1.0	08-06-2020	Opgesteld	Peter Kager (FG)
1.1	25-02-2021	Herzien/ definitief gemaakt	Dimmen Smolders (FG)
1.2	21-05-2021	Kleine herziening nav input directie-overleg	Dimmen Smolders (FG)
	xx-xx-2020	Instemming	Medezeggenschapsraad
	xx-xx-2020	Vastgesteld	Bestuur

Inhoudsopgave

Inleiding

Een intern privacybeleid is bedoeld om uit te leggen hoe we bij Delta-onderwijs omgaan met persoonsgegevens. Het gaat daarbij niet alleen om een naam of contactgegevens, maar soms hebben we ook te maken met bijzondere persoonsgegevens zoals de gezondheid van een leerling. Wij willen graag zorgvuldig omgaan met de persoonsgegevens van onze leerlingen. En daarom is het van belang dat we een beleid daarvoor hanteren.

Daarnaast digitaliseert onderwijs steeds meer, er wordt veelvuldig gebruik gemaakt van computers en bepaalde computerprogramma's. Ook daar moeten we binnen Delta-onderwijs op een goede manier mee omgaan. In deel 2 van dit interne privacybeleid lees je hoe we met ICT-bedrijfsmiddelen om moeten gaan.

Tot slot zijn we ook verplicht om goed met persoonsgegevens van alle medewerkers om te gaan. Als werkgever verwerken wij immers verschillende persoonsgegevens. We hebben niet alleen bepaalde gegevens nodig om het salaris uit te kunnen betalen, maar denk ook aan contactgegevens voor noodgevallen. In deel 3 van dit document leggen we uit welke persoonsgegevens wij van medewerkers verwerken en waarom we dat doen.

Dit intern privacybeleid bestaat uit drie delen. Deel 1 gaat over het verwerken van persoonsgegevens van leerlingen. In deel 2 staan we stil bij het veilig gebruiken van ICT-bedrijfsmiddelen. Deel 3 betreft de interne privacyverklaring, waarin wordt uitgelegd hoe Delta-onderwijs met jouw persoonsgegevens omgaat.

ICTRECHT privacy

ICTRecht Privacy B.V.
Jollemanhof 12
1019 GW Amsterdam

TELEFOON
020 663 1941

E-MAIL
privacy@ictrecht.nl

INTERNET
ictrecht.nl/privacy

KVK
72602651

BTW
NL859169820B01

IBAN
NL64 RABO 0334 0962 94

Deel 1 – Privacyreglement

1. Rollen en verantwoordelijkheden

Voordat we uitleggen hoe we binnen Delta-onderwijs omgaan met persoonsgegevens van leerlingen, medewerkers en anderen is het van belang om te weten wie wat doet als het gaat om privacy. We geven hieronder een overzicht van de verschillende rollen, functies en taken. Een meer gedetailleerd overzicht van rollen en verantwoordelijken is te vinden in Bijlage 1 (pagina 17 van dit document).

Eindverantwoordelijk

De volgende rollen zijn eindverantwoordelijk voor dit intern privacybeleid:

- Schoolbestuur
- Voorzitter College van Bestuur
- Directeur

Directie en bestuur zijn niet alleen eindverantwoordelijk, maar ook de zogeheten verwerkingsverantwoordelijken. De verwerkingsverantwoordelijke bepaalt waarom er persoonsgegevens worden verzameld en hoe dat gebeurt.

Uitvoering

Verschillende rollen zijn verantwoordelijk dat dit beleid ook daadwerkelijk wordt nageleefd:

- ICT-coördinator
- ICT-beheerder
- Functioneel beheerder
- Informatiemanager
- Security Officer
- Leidinggevenden

Toezicht en advies

De functionaris gegevensbescherming (FG) controleert of de privacywet, Algemene verordening gegevensbescherming (AVG) binnen Delta-onderwijs wordt nageleefd. Bij de FG kunnen we terecht met vragen op het gebied van privacy. De FG is ook betrokken bij incidenten en klachten.

Instemming

Maatregelen die direct betrekking hebben op de privacy van leerlingen of medewerkers kunnen niet worden uitgevoerd zonder instemming van de (gemeenschappelijke) medezeggenschapsraad. Zo hebben we voor dit intern privacybeleid eveneens instemming gevraagd van de GMR.

2. Begrippen

In dit privacyreglement gebruiken we verschillende begrippen die te maken hebben met privacy. Sommige begrippen zijn abstract, waardoor het niet altijd duidelijk is wat ermee wordt bedoeld. Daarom hebben we de meest voorkomende begrippen hieronder uitgelegd.

Bijzondere persoonsgegevens:	een persoonsgegeven dat iets zegt over iemand zijn ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische of biometrische gegevens, gegevens over de gezondheid, en gegevens over seksuele gerichtheid of seksueel gedrag.
Persoonsgegeven:	alle informatie over een natuurlijke persoon die ervoor kan zorgen dat hij/zij direct of indirect identificeerbaar is, of geïdentificeerd kan worden.
Verwerking van persoonsgegevens:	alles wat met persoonsgegevens gedaan wordt, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen of doorsturen.

3. Totstandkoming privacyreglement

3.1 Vaststellen privacyreglement

Dit privacyreglement is door het schoolbestuur vastgesteld, met instemming van de ouder/geleding van de gemeenschappelijke medezeggenschapsraad. De datum van vaststelling is opgenomen op het voorblad. Dit privacyreglement vervangt alle eerdere privacyreglementen.

3.2 Inwerkingtreding en duur privacyreglement

De regels die zijn vastgelegd in dit document gelden per direct. Het is mogelijk dat er wijzigingen worden aangebracht, bijvoorbeeld omdat er nieuwe inzichten zijn over hoe we met persoonsgegevens omgaan. Daarom kan dit privacyreglement van tijd tot tijd wijzigen.

3.3 Reikwijdte privacyreglement

Dit privacyreglement gaat over het verwerken van persoonsgegevens van leerlingen en in sommige gevallen ook van ouders, verzorgers of voogden. In dit privacyreglement heeft Delta-onderwijs een aantal regels vastgelegd ten aanzien van de omgang met deze persoonsgegevens.

3.4 Doel privacyreglement

Dit privacyreglement heeft verschillende doelen:

a. de privacy van leerlingen beschermingen tegen verkeerd en onbedoeld gebruik van persoonsgegevens;
b. toelichten welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt;
c. zorgvuldige verwerking van persoonsgegevens te waarborgen; en
d. de rechten van leerlingen te waarborgen.

4. Verplichtingen van Delta-onderwijs

De AVG, legt verschillende verplichtingen op aan organisaties die persoonsgegevens verwerken. Zo heeft Delta-onderwijs in het kader van privacy ook diverse verplichtingen:

- Op een zorgvuldige, veilige en vertrouwelijke manier omgaan met persoonsgegevens.
- Ouders en leerlingen informeren over onder andere wat wij doen met hun persoonsgegevens en welke rechten zij hebben.
- Het sluiten van verwerkersovereenkomsten met alle leveranciers van digitale onderwijsmiddelen, indien de leveranciers in opdracht van Delta-onderwijs persoonsgegevens verwerken.
- Het aanstellen van een FG, die erop toeziet dat de AVG en aanverwante regelgeving wordt nageleefd. Mocht je vragen of klachten hebben op het gebied van privacy, dan kun je daarvoor terecht bij onze FG via d.smolders@ictrecht.nl.
- Beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan betrokkenen.
- Ervoor zorgen dat de persoonsgegevens op een juiste wijze beveiligd zijn. Hiervoor lees je meer in de Gedragscode ICT-bedrijfsmiddelen.

5. Soorten persoonsgegevens

Delta-onderwijs verwerkt verschillende persoonsgegevens van leerlingen, maar ook van ouders, verzorgers of voogden. Deze gegevens zijn nodig om onderwijs te kunnen geven. In de AVG wordt onderscheid gemaakt tussen persoonsgegevens en bijzondere persoonsgegevens. Hieronder is opgesomd welke (bijzondere) persoonsgegevens verwerkt kunnen worden.

5.1 Persoonsgegevens

Binnen Delta-onderwijs worden alleen persoonsgegevens verwerkt voor zover dat nodig is. Hebben we bepaalde gegevens niet meer nodig, dan zorgen we ervoor dat die verwijderd worden. In ons dataregister houden wij een overzicht bij van alle persoonsgegevens die verwerkt worden.

5.2 Bijzondere persoonsgegevens

In principe is het verwerken van bijzondere persoonsgegevens verboden. Binnen Delta-onderwijs doen wij dit alleen als er een uitzondering is op basis waarvan we toch deze gegevens mogen verwerken.

Zo kunnen er gezondheidsgegevens verwerkt worden. Denk bijvoorbeeld aan een leerling die een notenallergie heeft.

5.3 Wijze van verkrijgen van persoonsgegevens

De meeste persoonsgegevens worden verstrekt wanneer een leerling wordt aangemeld. Gegevens kunnen ook worden verkregen via de vorige onderwijsinstelling of opvang waar de leerling ingeschreven was.

6. Verwerken van persoonsgegevens

Als we persoonsgegevens verwerken, dan moeten we ons houden aan een aantal basisregels. Daarnaast moeten we erop letten dat de juiste overeenkomsten worden gesloten met de verschillende partijen waar we mee samenwerken indien die partijen persoonsgegevens van onze leerlingen en/of medewerkers verwerken.

6.1 Basisregels bij het omgaan met persoonsgegevens

Wanneer we persoonsgegevens verwerken, moeten we rekening houden met een aantal basisregels die in de AVG zijn vastgelegd:

- Rechtmatigheid, behoorlijkheid en transparantie
  Delta-onderwijs is verplicht om leerlingen, ouders, verzorgers en/of voogden, maar ook werknemers uit te leggen in hoeverre en op welke manier persoonsgegevens worden verwerkt.

- Doelbinding
  Persoonsgegevens mogen alleen gebruikt worden voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Bijvoorbeeld voor het geven van passend onderwijs.

- Dataminimalisatie
  Delta-onderwijs mag niet meer persoonsgegevens verwerken dan noodzakelijk is om dat doel te bereiken. Het is bijvoorbeeld niet noodzakelijk om te weten welke schoenmaat een leerling heeft om hem of haar onderwijs te kunnen geven.

- Juistheid
  De persoonsgegevens die Delta-onderwijs verwerkt, moeten juist en actueel zijn.

- Opslagbeperking
  Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk. In het dataregister zijn bewaartermijnen opgenomen. Zijn de persoonsgegevens niet meer nodig, of is de bewaartermijn verstreken, dan moeten de persoonsgegevens verwijderd worden.

- Integriteit en vertrouwelijkheid
  Delta-onderwijs dient technische en organisatorische beveiligingsmaatregelen te nemen om ongeoorloofde toegang tot of het ongeoorloofde gebruik van persoonsgegevens te voorkomen.

6.2 Doeleinden

Persoonsgegevens worden verwerkt voor onder meer de volgende doeleinden:

- Het geven en organiseren van het onderwijs
  - geven van onderwijs en de begeleiding van leerlingen;
  - verstrekken of ter beschikking stellen van leermiddelen;
  - informeren van ouder(s), verzorger(s) en/of voogd(en) over de vorderingen van de leerling en over activiteiten op school;
  - administratie van bijdragen of vergoedingen voor leermiddelen, en vrijwillige ouderbijdragen.

- Nakomen van een wettelijke plicht
    - laten uitvoeren van accountantscontrole;
    - voldoen aan de vraag gegevens te verstrekken aan organisaties zoals de gemeente en overheid;
    - voldoen aan de vraag gegevens te verstrekken aan het samenwerkingsverband passend onderwijs, voor advies, ondersteuning of het beoordelen van de toelaatbaarheid van de leerling tot speciaal onderwijs.
- Zorgen voor veiligheid op school
    - onderzoeken en vastleggen van gezondheidsrisico's en gedrag rondom (het voorkomen van) pesten;
    - registreren en afhandelen van klachten (vertrouwenspersoon);
    - registreren van medische condities van leerlingen waar medewerkers rekening mee moeten houden;
    - gegevensregistratie ten behoeve van calamiteiten(bestrijding);
    - uitvoeren van videocameratoezicht.

6.3 Grondslag voor verwerking van persoonsgegevens

Delta-onderwijs mag alleen persoonsgegevens verwerken als daar een wettelijke grondslag voor is. In de AVG zijn de grondslagen vermeld:

- Toestemming
    - Denk daarbij aan het publiceren van foto's op de website.
- Uitvoering van de overeenkomst
    - Voor het geven van onderwijs aan de leerling zijn persoonsgegevens nodig.
- Voldoen aan een wettelijke plicht
    - Delta-onderwijs is gebonden aan onderwijswetgeving op basis waarvan in bepaalde situaties persoonsgegevens aan derde partijen moeten worden verstrekt. Denk daarbij aan een leerplichtambtenaar.
- Bescherming van vitale belangen
    - Denk aan het verwerken van medische gegevens bij een ongeluk.
- Taak van algemeen belang
    - Delta-onderwijs is verantwoordelijk voor het geven van onderwijs. Dit betekent dat persoonsgegevens aan externe partijen kunnen worden verstrekt als dit noodzakelijk is.
- Gerechtvaardigd belang
    - Wanneer Delta-onderwijs de grondslag "gerechtvaardigd belang" gebruikt voor het verwerken van persoonsgegevens, dan dient er een belangenafweging te worden gemaakt. Het gaat daarbij om het belang van Delta-onderwijs vs. het privacybelang van de leerling.

6.4 Schriftelijke afspraken over verwerken van persoonsgegevens

Wanneer Delta-onderwijs persoonsgegevens verwerkt, kunnen daar andere partijen bij betrokken zijn. Denk bijvoorbeeld aan het gebruiken van bepaalde computerprogramma's, of een leerlingenadministratie. Het bedrijf daarachter krijgt inzage in de persoonsgegevens van leerlingen.

Daarnaast is Delta-onderwijs in sommige gevallen verplicht om persoonsgegevens van leerlingen te delen met andere organisaties. Denk bijvoorbeeld aan de situatie waarin de leerling van de ene school overstapt naar een andere school. Daarnaast worden persoonsgegevens in ieder geval verstrekt aan onderstaande instanties:

- Ministerie van Onderwijs, Cultuur en Wetenschappen;
- Onderwijsinspectie;
- Gemeente;
- Samenwerkingsverband passend onderwijs.

Wanneer Delta-onderwijs persoonsgegevens verstrekt aan of verkrijgt van een andere organisatie, dan heeft Delta-onderwijs afspraken gemaakt over onder andere de inzage of uitwisseling, maar ook beveiliging van de persoonsgegevens van leerlingen.

7. Beveiliging van persoonsgegevens

7.1 Toegang tot de persoonsregistratie en beveiliging

Delta-onderwijs neemt alle technische en organisatorische beveiligingsmaatregelen die nodig zijn om te voorkomen dat de persoonsgegevens op de verkeerde plek terecht komen of dat de persoonsgegevens ingezien worden door mensen die deze gegevens niet nodig hebben voor hun werk. Zo hebben alleen bepaalde medewerkers inzage en toegang tot een leerlingendossier.

Iedereen die binnen Delta-onderwijs persoonsgegevens verwerkt, is verplicht daar vertrouwelijk mee om te gaan. Delta-onderwijs heeft een aparte gedragscode opgesteld over beveiliging en het gebruik van ICT-bedrijfsmiddelen.

7.2 Bewaren en verwijderen van persoonsgegevens

Onderdeel van beveiliging is dat Delta-onderwijs zich houdt aan bewaartermijnen en persoonsgegevens verwijdert indien die niet meer nodig zijn. Hoe minder persoonsgegevens Delta-onderwijs heeft van een leerling, hoe kleiner de kans dat daar ook iets mee gebeurt.

Delta-onderwijs moet zich houden aan verschillende bewaartermijnen. Zo is Delta-onderwijs wettelijk verplicht om de gegevens van leerlingen 5 jaar lang in de administratie te bewaren. Deze termijn gaat lopen vanaf het moment dat de leerling de school heeft verlaten. Gegevens waar geen specifieke bewaartermijn voor geldt, worden na 2 jaar vernietigd.

Een overzicht van bewaartermijnen is te vinden in het dataregister.

8. Datalekken

Ondanks alle beveiligingsmaatregelen kan het voorkomen dat er iets gebeurt met persoonsgegevens wat niet de bedoeling was. Dat kan resulteren in een datalek. Een datalek is:

> *een inbreuk op de beveiliging die* ***per ongeluk of op onrechtmatige wijze*** *leidt tot de* ***vernietiging****, het* ***verlies****, de* ***wijziging*** *of de ongeoorloofde* ***verstrekking*** *van of de ongeoorloofde* ***toegang*** *tot doorgezonden, opgeslagen of anderszins verwerkte* ***gegevens****.*

In het kort: alles wat 'verkeerd gaat' met persoonsgegevens. Een datalek ligt altijd op de loer wanneer persoonsgegevens worden verwerkt. Fouten maken is immers menselijk. Het belangrijkste is dan ook dat we een datalek op de juiste manier afhandelen, mocht het voorkomen.

Voorbeelden van datalekken zijn:

- Het versturen van een e-mailbericht waarbij de ontvangers in de 'cc' staan, terwijl zij elkaars e-mailadres niet behoren te kennen (deze moeten dus in de 'bcc');
- Ouder van leerling A per ongeluk informeren over de ziekte van leerling B;
- Persoonsgegevens van leerlingen verspreiden buiten de organisatie, terwijl je ze intern wilde delen.

Meer informatie over datalekken hebben we opgenomen in ons calamiteitenplan datalekken.

9. Rechten van de leerlingen, ouders, verzorgers en/of voogden

In de AVG zijn diverse rechten opgenomen. Zolang de leerling de leeftijd van 16 jaar nog niet heeft bereikt, is het aan de ouders, verzorgers en/of voogden om de rechten uit te oefenen.

Indien een verzoek tot uitoefening van een van de rechten wordt ingediend bij Delta-onderwijs, dient daar binnen 1 maand op te worden gereageerd. Indien het verzoek dermate veelomvattend is dat er meer tijd nodig is, dan mag de termijn met 2 maanden verlengd worden.

Wanneer een verzoek wordt ingediend, dan is het van belang om er zeker van te zijn dat de juiste gegevens worden verstrekt aan de juiste persoon. Daarom mag Delta-onderwijs de ouders en/of leerlingen vragen om zich te identificeren.

9.1 Recht op inzage

De ouders en leerling hebben het recht om te weten welke persoonsgegevens worden verwerkt door Delta-onderwijs. Wanneer een inzageverzoek wordt ingediend, is het aan Delta-onderwijs om te verifiëren welke persoonsgegevens er zijn van de desbetreffende leerling, en vervolgens een kopie daarvan te verstrekken.

9.2 Recht op rectificatie

Wanneer de gegevens niet juist zijn, dan bestaat er het recht om de gegevens te laten corrigeren. Bijvoorbeeld in geval van een verhuizing, dan moeten de nieuwe adresgegevens worden doorgegeven.

9.3 Recht op verwijdering

Los van het feit dat Delta-onderwijs verplicht is om persoonsgegevens te verwijderen indien die niet langer meer nodig zijn, bestaat er ook het recht om uit de systemen van Delta-onderwijs verwijderd te worden. Delta-onderwijs kan alleen aan het verzoek voldoen als de gegevens inderdaad niet meer nodig zijn. In sommige gevallen geldt namelijk een wettelijke bewaartermijn, en in dat geval mogen de persoonsgegevens niet verwijderd worden binnen die termijn.

9.4 Recht op beperking van de verwerking

De ouders en leerling kunnen Delta-onderwijs vragen om tijdelijk geen gegevens van de leerling te gebruiken. De gegevens worden dan tijdelijk ‘bevroren’. Dit kan bijvoorbeeld als er discussie is over de juistheid van de gegevens of wanneer er bezwaar is gemaakt tegen het gebruik van persoonsgegevens.

9.5 Recht op dataportabiliteit

Er bestaat een recht om Delta-onderwijs te vragen om de persoonsgegevens over te dragen aan een andere organisatie. Denk aan de situatie waarin de leerling de school verlaat en naar een andere school gaat. Dan kan er een verzoek worden ingediend om bijvoorbeeld het leerlingendossier over te dragen.

9.6 Recht van bezwaar

Wanneer Delta-onderwijs persoonsgegevens verwerkt op basis van een taak van algemeen belang of gerechtvaardigd belang, dan moet er een belangenafweging worden gemaakt ten aanzien van de privacybelangen van de leerling. Wanneer

Delta-onderwijs besluit dat de persoonsgegevens verwerkt mogen worden, en het privacybelang van de leerling minder groot is dan het belang van Delta-onderwijs, dan kan er bezwaar worden gemaakt. Het bezwaar moet wel onderbouwd zijn, en Delta-onderwijs zal vervolgens nogmaals een belangenafweging maken.

9.7 Geautomatiseerde individuele besluitvorming (profiling)

Delta-onderwijs zal geen besluiten nemen over leerlingen die uitsluitend gebaseerd zijn op geautomatiseerde verwerking van gegevens (ook niet door gebruik te maken van profiling). De computer neemt op school dus niet zomaar onderwijskundige, geautomatiseerde beslissingen die gevolgen kunnen hebben voor de privacy van de leerlingen.

9.8 Klacht indienen

Delta-onderwijs doet er alles aan om de privacy van de leerlingen te waarborgen. Indien ouders, verzorgers, voogden en/of leerlingen van mening zijn dat er niet op de juiste manier wordt omgegaan met de persoonsgegevens, dan is er een mogelijkheid om een klacht in te dienen.

Allereerst kan er een klacht ingediend worden bij onze FG via d.smolders@ictrecht.nl. Ten tweede bestaat er altijd de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Bijlage 1 Rollen en verantwoordelijkheden

Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij Delta-onderwijs

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Bestuur / Directie	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Intern privacybeleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	Privacy officer (directielid Delta-onderwijs)	• Inhoudelijk verantwoordelijk voor intern privacybeleid • Controle intern privacybeleid • Adviseert bestuur/directie over intern privacybeleid • Voorbereiden uitvoeren intern privacybeleid Classificatie/risicoanalyse • Evalueren intern privacybeleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Processen, richtlijnen en procedures intern privacybeleid, waaronder: • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor gegevens-bescherming	• Toezicht op naleving privacy wetgeving • Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Intern privacybeleid • Inrichten meldpunt datalekken
	Schooldirecteur / Verantwoordelijken voor o.a.: ICT, HRM / P&O, facilitair, onderwijs,	• Classificatie / risicoanalyse in samenwerking met de privacy officer en FG • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/directie	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister • Classificatie- en risicoanalyse documenten.

	financiën, inkoop en administratie	• Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
Uitvoerend (operationeel)	Privacy officer Dagelijkse leiding / leidinggevende / directie	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken

Deel 2 – Gedragscode bedrijfsmiddelen

1. Inleiding

Het gebruik van internet, computernetwerk, en e-mail is voor alle medewerkers van de stichting noodzakelijk om de werkzaamheden te kunnen verrichten. Bij deze werkzaamheden wordt gebruik gemaakt van veel gegevens, waaronder persoonsgegevens. De (ICT-)faciliteiten en de verschillende gegevens worden in dit document **bedrijfsmiddelen** genoemd.
Onder bedrijfsmiddelen worden in ieder geval verstaan:

- Hardware: pc, laptop, tablet, telefoon, hardware token (tag), druppel.
- Software (of -systemen): alle applicaties voor het uitvoeren van de werkzaamheden, zoals de school e-mailomgeving, Microsoft Office, administratiesystemen en (online)digitaal lesmateriaal maar ook apps op (mobiele) apparaten.
- Informatie en (persoons)gegevens: rapportages, leerlingendossiers, gegevens in e-mails. Hierbij vraagt de verwerking van persoonsgegevens vanuit de privacywetgeving extra maatregelen.
- Internetgebruik: het bezoeken van het World Wide Web, het gebruik van e-mail en sociale media.

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers van Delta-onderwijs wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor de school uit te voeren.

De afspraken in dit document gelden voor alle locaties van waaruit (school)werkzaamheden worden verricht en voor alle apparaten waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij Delta-onderwijs.

1.1 Uitgangspunten gedragscode

Deze gedragscode legt regels vast voor het gebruik van de bedrijfsmiddelen door medewerkers en over de controle op de naleving hiervan.
Het doel van deze gedragscode is om de normen en uitgangspunten vast te leggen ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
- het tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
- de bescherming van privacy gevoelige informatie waaronder persoonsgegevens van het schoolbestuur, haar medewerkers, leerlingen en hun ouders en daarmee het beschermen van de privacy en veiligheid van alle betrokkenen;
- de bescherming van vertrouwelijke informatie van het schoolbestuur, haar medewerkers, leerlingen en hun ouders;
- het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen;
- de bescherming van de intellectuele eigendomsrechten van het schoolbestuur en derden;
- het voorkomen van negatieve publiciteit;
- kosten- en capaciteitsbeheersing.

De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. Delta-onderwijs zal dan ook de controle en handhaving van deze regels conform de privacywetgeving en het algemene arbeidsrechtelijk kader uitvoeren. Hierbij is het uitgangspunt een goede balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers op de werkplek. Gegevens worden alleen verzameld en gebruikt voor deze doelen. In het bijzonder zal het bestuur de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang.

1.2 Eigen verantwoordelijkheid en privégebruik

Het gebruik van door Delta-onderwijs verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle apparaten die voor schoolwerk worden gebruikt (inclusief eigen apparaten, oftewel 'Own Device') worden niet uitgeleend of aan anderen ter beschikking gesteld zonder aanvullende (beveiligings)maatregelen. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen.

1.3 Verschillende soorten gegevens

Delta-onderwijs is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens.

Delta-onderwijs onderscheidt drie typen gegevens:

- Openbare gegevens; dit zijn gegevens die juist voor publicatie bedoeld zijn.
- Interne gegevens; dit zijn gegevens die alleen voor gebruik en verwerking binnen Delta-onderwijs bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- Vertrouwelijke gegevens; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen Delta-onderwijs toegankelijk zijn. Denk hierbij aan (bijzondere) persoonsgegevens of personeelsgegevens.

Persoonsgegevens verdienen bijzondere aandacht. Dit zijn gegevens die een persoon betreffen én waardoor een persoon geïdentificeerd of identificeerbaar is. Denk hierbij aan naamgegevens, e-mailadressen maar ook telefoonnummers van zowel collega's als leerlingen en ouders van leerlingen.

De privacywetgeving verplicht de stichting om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat Delta-onderwijs schriftelijk afspraken maakt met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk).

Delta-onderwijs heeft een functionaris gegevensbescherming aangesteld. Deze communiceert intern de gedragsregels die horen bij het verwerken van persoonsgegevens. Persoonsgegevens moeten altijd met uiterste zorgvuldigheid verwerkt en gedeeld worden.

Als persoonsgegevens toegankelijk en of inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot deze gegevens, is er sprake van een beveiligingsincident, waaruit een datalek kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en Delta-onderwijs. Hoe te handelen ingeval sprake is van een datalek is nader uitgewerkt in het calamiteitenplan datalekken.

Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt Delta-onderwijs afspraken over:

- De verwerking en verspreiding van vertrouwelijke- en persoonsgegevens. Er worden niet meer gegevens verwerkt dan noodzakelijk om het doel te bereiken;
- De uitwisseling van gegevens, waarbij aan de ontvanger wordt aangegeven wat de ontvanger wel of niet mag doen met de gegevens;
- Opslag en verspreiding van gegevens, waarbij alléén gebruik gemaakt wordt van door Delta-onderwijs goedgekeurde bedrijfsmiddelen.

Van medewerkers van Delta-onderwijs en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bijvoorbeeld leerlingdossiers of andere vertrouwelijke gegevens, wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. Daarnaast wordt van hen verwacht dat zij de privacywetgeving hanteren en op geen enkele wijze informatie, waarvan redelijkerwijze kan worden aangenomen dat deze vertrouwelijk of privacygevoelig is, zonder toestemming van betrokkenen of leidinggevenden gebruiken en/of naar buiten te brengen.

2. Gedragscode

In deze gedragscode voor verantwoord gebruik van bedrijfsmiddelen geeft Delta-onderwijs aan wat de afspraken zijn met betrekking tot verschillende onderwerpen rondom het gebruik van bedrijfsmiddelen en wat dit voor de medewerkers in de dagelijkse praktijk betekent.

2.1 Algemene normen

Iedere medewerker voldoet aan de volgende algemene normen voor 'zorgvuldigheid' (niet uitputtend):

- Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht;
- Voorkom het lekken van interne en vertrouwelijke informatie;
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen;
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild;
- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering bij je directeur.

2.2 Computergebruik

Voor het uitoefenen van de werkzaamheden stelt Delta-onderwijs aan de medewerker computer- en netwerkfaciliteiten (ICT-bedrijfsmiddelen) ter beschikking. Het gebruik van deze ICT-bedrijfsmiddelen is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden;
- Weet welke gegevens er mogen worden gebruikt (mag iedereen het zien?) en welke ICT-voorzieningen kunnen worden ingezet (is het veilig genoeg?) bij het verrichten van de verschillende schoolwerkzaamheden;
- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op. (Opslaan van gegevens in public Cloud omgevingen, zoals een persoonlijke dropbox, is niet toegestaan);
- Versleutel alle gegevens met betrekking tot Delta-onderwijs, indien deze gegevens, om welke reden dan ook, elders opgeslagen worden (denk hierbij ook aan een usb-stick);
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk;
- Sluit na gebruik de computer af of log uit;
- Meld storingen van beheerde werkplekken (computer of laptop) bij je directeur.

2.3 Werkplek

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen waartoe zij geen rechten hebben en/of laat gegevens niet (onbedoeld) lekken. Als aanvullende regels op computergebruik gelden voor de werkplek de volgende clean desk- en schermvergrendelingsregels:

- Vergrendel bij het tijdelijk verlaten van de werkplek de pc;
- Verwijder interne en vertrouwelijke documenten, zoals een registratiemap, van het bureau bij het voor langere tijd verlaten van de werkplek (denk hieraan bij het bijwonen van een vergadering);
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via een beamer) mee kan kijken. Sluit het e-mailprogramma af en zorg voor een opgeruimd digitaal bureaublad;
- Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan;
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar of deponeer deze in daarvoor bestemde containers.

LET OP: Als persoonsgegevens toegankelijk/inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot die gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Weet dat beveiligingsincidenten en mogelijke datalekken gemeld moeten worden volgens de procedure die is vastgelegd in het calamiteitenplan datalekken.

2.4 Gebruik eigen apparaten (BYOD)

Beveiligingsmaatregelen hebben betrekking op alle apparaten waarmee werkzaamheden voor Delta-onderwijs worden uitgevoerd. Delta-onderwijs is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school.

Voor ‘Own Devices’ ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

- Beveilig het apparaat met een sterk wachtwoord of pincode;
- Vergrendel het apparaat bij het verlaten van de werkplek;
- Sla persoonsgegevens van Delta-onderwijs bij voorkeur niet op het eigen apparaat op. Als het toch moet, verwijder de persoonsgegevens na gebruik dan direct;
- Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot Delta-onderwijs, als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden (denk hierbij aan het eigen device of usb-stick);
- Scheid (versleutelde) gegevens, anders dan persoonsgegevens, van Delta-onderwijs en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen apparaat;
- Houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks);
- Neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het periodiek (minimaal maandelijks) scannen van het device.

Delta-onderwijs mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van Delta-onderwijs moet de medewerker zelf aantonen dat de bovenstaande maatregelen worden toegepast.

2.5 Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal is niet meer weg te denken bij Delta-onderwijs. Dit lesmateriaal staat steeds meer online waarbij steeds vaker persoonsgegevens worden uitgewisseld. De privacywetgeving eist dat elke organisatie vooraf aan het gebruik van dergelijk materiaal bekijkt wat de invloed ervan is op de privacy, dit kan specifieke maatregelen tot gevolg hebben.

De onderstaande regels gelden voor installatie en gebruik van software en (online) digitaal lesmateriaal:

- Installeren van software wordt bij Delta-onderwijs alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen;
- Bij het gebruik van online software, apps en digitaal lesmateriaal, wordt gekeken of er persoonsgegevens bij verwerkt worden;
- Een verwerkersovereenkomst wordt afgesloten met elke leverancier van (online)software, die in opdracht van Delta-onderwijs persoonsgegevens verwerkt. Regel dit voorafgaand aan het gebruik;
- Aanvragen van digitaal lesmateriaal en/of andere software volgt bij Delta-onderwijs via de afgesproken aanvraagprocedure.

2.6 Gebruik van e-mail

Delta-onderwijs stelt een e-mailsysteem en een bijbehorende mailbox aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik van e-mailfaciliteiten is verbonden aan deze werkzaamheden en gaan uit van de volgende afspraken:

- Gebruik het school e-mailadres alléén voor school gerelateerde zaken;
- Gebruik voor privé e-mail een eigen privé e-mailadres via een externe webmaildienst (bijvoorbeeld webmail van Gmail, Hotmail of een eigen provider);
- Ontvangen van privémail op het school e-mailadres is incidenteel toegestaan;
- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie;
- Het is niet toegestaan e-mail te gebruiken voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of voor berichten die kunnen aanzetten tot haat en geweld;
- Synchroniseert een medewerker de school e-mail met eigen apparaten (tablet, telefoon) dan kan Delta-onderwijs, bij verlies of diefstal van het apparaat, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het apparaat gewist worden.

2.7 Gebruik van internet

Delta-onderwijs stelt het gebruik van internet en de bijbehorende faciliteiten aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik hiervan is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Beperkt persoonlijk gebruik is toegestaan, mits dit:
  - niet storend is voor de dagelijkse werkzaamheden;
  - niet voor commerciële doeleinden is; en
  - geen verboden gebruik oplevert.
- Het is niet toegestaan om
  - websites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
  - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron;
  - onder lestijd internettoegang te gebruiken voor privédoeleinden;
  - deel te nemen aan kansspelen.
- Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale netwerken en andere vergelijkbare communicatienetwerken over alle aan school verbonden betrokkenen en activiteiten. Dit geldt in het bijzonder ook voor internetgebruik buiten het schoolnetwerk met betrekking tot aan de school verbonden betrokkenen en activiteiten.

2.8 Veilig online

We brengen met z'n allen steeds meer tijd online door. Hierbij worden steeds meer mobiele apparaten gebruikt. Menselijk gedrag staat veelal aan de basis van een datalek.

Delta-onderwijs verwacht van medewerkers dat zij:

- het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken) en websites;
- bij het verwerken van persoonsgegevens alléén gebruik maken van bekende én beveiligde draadloze netwerken;
- weten wat malware is, het kunnen herkennen en weten hoe te handelen;
- terughoudend zijn met het online achterlaten van gegevens met betrekking tot Delta-onderwijs;
- controleren of er daadwerkelijk van een bekend én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes. (Een netwerk kan bekend zijn, omdat het een netwerk van Delta-onderwijs of het eigen draadloze netwerk thuis is).

2.9 Sociale media

Sociale media is een verzamelnaam voor alle internettoepassingen die het mogelijk maken om informatie met elkaar te delen op een eenvoudige en vaak leuke manier. Het gaat hierbij niet alleen om informatie in de vorm van tekst (nieuws, artikelen). Ook geluid (podcasts, muziek) en beeld (fotografie, video) worden gedeeld via sociale media (Instagram, YouTube, Facebook, Twitter enz). De essentie van sociale media is dat iemand er informatie deelt over zichzelf, over anderen of over een bepaald onderwerp.

Voor het gebruik van sociale media geldt als uitgangspunt dat het digitale gedrag hierop niet afwijkt van het real life gedrag binnen de school. Medewerkers zijn altijd de vertegenwoordiger van Delta-onderwijs, ook als zij online een privémening verkondigen.

Bij Delta-onderwijs gelden de volgende afspraken voor het gebruik van sociale media:

- Deel op verantwoorde wijze kennis via sociale media, rekening houdend met de goede naam van Delta-onderwijs en iedereen die hierbij betrokken is;
- Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens Delta-onderwijs gedaan wordt;
- Publiceer geen vertrouwelijke informatie op sociale media;
- Publiceer geen beeldmateriaal van leerlingen zonder de uitdrukkelijke voorafgaande aantoonbare toestemming van ouders (als de leerling jonger is dan 16 jaar) of de leerling zelf (als deze ouder dan 16 jaar is);
- Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn. Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren;
- Neem contact op met een leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met Delta-onderwijs;
- Het inzetten van sociale media in het lesprogramma is gebonden aan de toestemming van ouders als leerlingen jonger zijn dan 16 jaar.

2.10 Gebruik beeld- en geluidsmateriaal

Het gebruiken van beeld- en geluidsmateriaal, het delen van foto's, video's en geluidsfragmenten van leerlingen door medewerkers vallend onder Delta-onderwijs, mag alleen als daar vooraf toestemming voor gegeven is door ouders (als de leerling jonger is dan 16 jaar) of de leerling zelf (als deze ouder dan 16 jaar is). Zonder deze toestemming mogen geen foto's, video's en geluidsfragmenten van leerlingen gebruikt worden.

- Delta-onderwijs legt in de aanmeldformulieren de voornoemde toestemming per leerling vast. Ouders/leerlingen kunnen te allen tijde hun toestemming aanpassen. Medewerkers dienen voorafgaand aan het gebruiken/delen van foto's, video's en geluidsfragmenten van leerlingen het formulier te raadplegen of hiervoor toestemming is verleend;
- Voor de afspraken rondom het delen van beeld- en geluidsmateriaal via sociale media gelden de richtlijnen die genoemd worden bij het gebruik van sociale media.

2.11 Wachtwoorden en pincodes

Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en apparaten (pc, laptop, telefoon) begint met een goed wachtwoord. Een lang wachtwoord of een 'wachtzin' is beter dan een kort, complex wachtwoord. Voor het gebruik van wachtwoorden gelden onderstaande afspraken:

- Wachtwoorden moeten, waar mogelijk, minimaal 9 tekens bevatten, met minstens drie van de volgende vier elementen: kleine letter, hoofdletter, cijfer of speciaal teken (!@#$%^&*()\);

- Pincodes (op telefoon of tablet) moeten, waar mogelijk, langer zijn dan 4 tekens;
- Wachtwoorden moeten volgens de afspraken binnen Delta-onderwijs op aangegeven tijden vervangen worden;
- Gebruik niet voor elk systeem hetzelfde wachtwoord;
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.

2.12 Meldplicht Datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens de procedure meldplicht datalekken van Delta-onderwijs.

3. Controle gebruik bedrijfsmiddelen

Delta-onderwijs handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving.

Delta-onderwijs zal bij controle rondom het gebruik van bedrijfsmiddelen, op basis van deze gedragscode, uitgaan van de juiste balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers.

3.1 Voorwaarden voor controle

- Controle van persoonsgegevens met betrekking tot gebruik van bedrijfsmiddelen vindt slechts plaats in het kader van handhaving van de doelen van deze gedragscode;
- Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen;
- Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode, in opdracht van Delta-onderwijs gerichte controle plaatsvinden;
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van Delta-onderwijs, controle op de inhoud plaats;
- Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt;
- Bij constatering van ongeoorloofd gebruik, wordt dit onmiddellijk door de leidinggevende met de betrokken medewerker besproken. Delta-onderwijs zal de medewerker, op verzoek, inzage verschaffen in de gegevens over het eigen gebruik. De medewerker wordt gewezen op de consequenties wanneer niet wordt gestopt met het ongeoorloofd gebruik;
- E-mailberichten van leden van de GMR onderling, van vertrouwenspersonen, bedrijfsartsen en van eenieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Dit geldt niet voor de veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.

3.2 Uitvoering van de controle

- De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering;
- De controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek;
- De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens;
- Controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is;
- De afdeling ICT en de systeembeheerder(s) zijn aan geheimhouding gebonden als men om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit;

- Door Delta-onderwijs worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn;
- Door Delta-onderwijs worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

3.3 Disciplinaire maatregelen

Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het bestuur van Delta-onderwijs, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen. Hieronder vallen o.a. een waarschuwing/berisping, schadevergoeding, aangifte bij de politie, overplaatsing, schorsing en/of beëindiging van de arbeidsovereenkomst.

Medewerkers die zich niet aan deze gedragscode houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken. Zij krijgen daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. Medewerker en leidinggevende maken dan afspraken voor de toekomst en bepalen de mogelijke maatregelen bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in deze gedragscode bepaalde. Ook kan de toegang tot e-mail of internet worden beperkt of geheel worden afgesloten. Er worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

3.4 Bezwaar en beroep

Als de medewerker het niet eens is met de (voorgenomen) disciplinaire maatregel, dan kan daar in een aantal gevallen bezwaar en/of beroep tegen worden ingesteld. Dit is meestal geregeld in de arbeidsovereenkomst, regels rondom personeelszaken en/of de van toepassing zijnde CAO.

4. GMR

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle van het gedrag of de prestaties van medewerkers. Het medezeggenschapsorgaan (de GMR) heeft om deze reden instemmingsrecht. Dit orgaan heeft op [DATUM] ingestemd met de inhoud van deze gedragscode.

De organisatie kan deze gedragscode met instemming van de GMR wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering ervan aan de medewerkers bekend gemaakt.

5. Slotbepaling

Deze regeling wordt 2-jaarlijks geëvalueerd door Delta-onderwijs en de GMR. De eerstkomende evaluatie vindt plaats op [DATUM].

ICTRecht Privacy B.V.
Jollemanhof 12
1019 GW Amsterdam

TELEFOON
020 663 1941

E-MAIL
privacy@ictrecht.nl

INTERNET
ictrecht.nl/privacy

KVK
72602651

BTW
NL859169820B01

IBAN
NL64 RABO 0334 0962 94

Deel 3 – Interne privacyverklaring

In dit deel informeren wij jou over hoe Delta-onderwijs, in de rol van werkgever, omgaat met jouw persoonsgegevens. Jouw privacy is voor ons van groot belang.

1. Welke gegevens verwerken van jou?

In het kader van de arbeidsovereenkomst verwerken wij verschillende persoonsgegevens van onze werknemers. Hieronder vind je een opsomming van de gegevens die wij van je verwerken:

- NAW-gegevens
- Contactgegevens (e-mailadres en telefoonnummer)
- Geboortedatum- en plaats
- Nationaliteit
- Geslacht
- Verlof- en verzuimregistratie
- Kopie ID-bewijs inclusief BSN
- Beeldmateriaal
- Naam en contactgegevens partner
- Geboortedatum partner
- Burgerlijke staat
- Naam en geboortedatum kind(eren)
- Handtekening
- Financiële gegevens, zoals IBAN-nummer(s)
- Gegevens loonbeslag
- Correspondentie en inhoud zakelijke mailbox
- Inhoud van de arbeidsovereenkomst
- Functie
- Gegevens m.b.t. jouw arbeidsomstandigheden
- Gegevens m.b.t. jouw arbeidsvoorwaarden
- Gegevens m.b.t. personeelsbeoordeling en de loopbaanbegeleiding
- Gegevens m.b.t. pensioen
- Loonbelastingverklaring
- Inhoud personeelsdossier
- Camerabeelden
- Gegevens noodcontactpersoon
- Medische gegevens
- Verklaring omtrent gedrag (VOG)
- Loggegevens
- Gebruik van ICT- en netwerkverkeer
- Zwangerschaps-/ouderschapsverlof
- Gegevens omtrent ziekte (registratie /correspondentie bedrijfsarts/UWV)

1.1 Waarom verwerken wij jouw gegevens?

Wij gebruiken jouw persoonsgegevens voor de volgende doeleinden:

- Uitvoering geven aan de arbeidsovereenkomst of beëindiging van de arbeidsovereenkomst
  In principe valt hier alles onder waardoor wij ervoor kunnen zorgen dat je bij ons aan de slag kunt. Ook als jouw dienstverband eindigt hebben we in sommige gevallen je persoonlijke gegevens nog een enige tijd nodig, maar we bewaren de gegevens niet langer dan noodzakelijk. Dit doen wij om uitvoering te geven aan de arbeidsovereenkomst of om te voldoen aan onze wettelijke plicht. Denk daarbij aan:
  - het opstellen van jouw arbeidsovereenkomst;
  - leidinggeven en de begeleiding in je ontwikkeling;
  - uitvoering van HR-activiteiten (zoals personeelsadministratie, salarisadministratie, pensioenadministratie en verzuimregistratie);
  - het bieden van bedrijf medische en/of maatschappelijke zorg indien nodig;
  - uitvoering geven aan de arbeidsvoorwaarden.

- Interne controle, werkoverdracht en bedrijfsbeveiliging
  Wij hechten veel waarde aan beveiliging. Daarom beveiligen wij onze school en bedrijfsmiddelen met camera's, houden wij logbestanden van onze ICT-systemen bij en kunnen wij ICT- en netwerkverkeer monitoren van werknemers indien nodig. Ook kunnen wij bij beveiligingsincidenten loggegevens in onze systemen raadplegen, waaruit blijkt wanneer er bijvoorbeeld is ingelogd. Wij hebben een gerechtvaardigd belang om dit te doen (veiligheid), de inbreuk op jouw privacy houden we hierbij zo minimaal mogelijk. Je kunt altijd bezwaar maken tegen de verwerkingen van persoonsgegevens op basis van jouw specifieke situatie. Meer informatie over beveiliging vind je in de Gedragscode ICT-bedrijfsmiddelen.

- Het (laten) uitvoeren van een accountantscontrole
  Bij een accountantscontrole worden persoonsgegevens verwerkt bijvoorbeeld om de salarisadministratie te controleren. Dit doen wij omdat de wet dit van ons eist.

- Noodsituaties
  Mocht er iets met jou gebeuren onder werktijd, bijvoorbeeld een ongeval of acute ziekte, dan nemen wij contact op met de persoon die jij hebt opgegeven voor in noodsituaties. Wij doen dit omdat het noodzakelijk is om jouw vitale belangen te beschermen.

- Het gebruik van foto's
  Op onze website plaatsen we foto's van medewerkers en leerlingen. Zo kunnen we een indruk geven van de sfeer die bij ons op school hangt.

1.2 De grondslagen voor het verwerken van jouw persoonsgegevens

We mogen jouw persoonsgegevens alleen verwerken als er een wettelijke grondslag voor bestaat. Wij verwerken jouw gegevens alleen op basis van een van de volgende grondslagen:

- ter **uitvoering van de arbeidsovereenkomst** die we met je hebben gesloten, zoals ter uitbetaling van je salaris;
- in bepaalde gevallen hebben we ook een **wettelijke verplichting** om bepaalde gegevens te verzamelen en te bewaren, zoals een kopie van je identiteitsbewijs en je BSN;
- het komt voor dat wij gegevens nodig hebben omdat wij daar een **gerechtvaardigd belang** bij hebben. In dat geval hebben we een afweging gemaakt tussen ons bedrijfsbelang en jouw recht op privacy, zoals voor beveiligingsdoeleinden;
- in uitzonderingssituaties hebben we jouw gegevens nodig om jouw leven te beschermen. Er is dan een zogenoemd **vitaal belang**. Het gaat dan om levensbedreigende (nood)situaties. Denk bijvoorbeeld aan een acute beroerte;
- ook kunnen wij jouw gegevens verwerken als we daarvoor jouw **toestemming** hebben verkregen. Dit doen wij alleen als je ook echt een vrije keuze hebt en er geen negatieve gevolgen zijn als je geen toestemming geeft.

2. Beveiliging en bewaartermijnen

2.1 Beveiliging van persoonsgegevens

Beveiliging van persoonsgegevens is voor ons van groot belang. Wij zorgen ervoor dat je gegevens bij ons goed beveiligd zijn. We passen de beveiliging steeds aan en letten goed op wat er mis kan gaan. Gaat er ondanks dat toch iets mis? Zijn er gegevens kwijtgeraakt of openbaar gemaakt? Of twijfel je over de beveiliging? Meld dit dan direct bij de functionaris gegevensbescherming (FG), zodat we de juiste procedures in gang kunnen zetten.

Wij nemen in ieder geval de volgende maatregelen:

- Autorisatie: slechts enkele bevoegde medewerkers hebben toegang tot jouw persoonsgegevens;
- TSL/SSL-verbinding: we hanteren een beveiligde internetverbinding;
- Logging: wij maken gebruik van logging. Dat betekent dat we precies bijhouden wie wat met jouw persoonsgegevens doet;
- Software: persoonsgegevens worden alleen verwerkt via veilige software;
- Wachtwoordbeleid: wij hanteren een strikt wachtwoordbeleid.

Meer informatie over beveiliging vind je in onze Gedragscode ICT-bedrijfsmiddelen.

2.2 Bewaartermijnen

Zolang je bij ons in dienst bent, bewaren wij jouw gegevens. Maar ook bij uitdiensttreding zijn wij in sommige gevallen wettelijk verplicht om jouw gegevens langer te bewaren. Denk bijvoorbeeld aan loonstroken waarvoor een fiscale bewaarplicht geldt. Hieronder sommen we nog enkele voorbeelden op van persoonsgegevens die we een bepaalde termijn bewaren:

- het personeelsdossier bewaren wij tot maximaal 2 jaar na uitdiensttreding;
- de salarisadministratie bewaren wij 7 jaar vanaf het boekjaar (fiscale bewaarplicht);
- je NAW-gegevens, geboortedatum, BSN, maar ook andere gegevens voor de inkomstenbelasting en een scan van je ID-bewijs bewaren wij tot maximaal 5 jaar nadat je uit dienst bent (op basis van de Uitvoeringsregeling loonbelasting);
- camerabeelden bewaren wij tot maximaal 4 weken na de opname, tenzij wij de beelden nodig hebben als bewijs in bijvoorbeeld een rechtszaak;
- logging en monitoringsgegevens bewaren wij tot maximaal 1 jaar na verzameling.

Een volledig overzicht van bewaartermijnen vind je in ons dataregister.

3. Derde partijen

Wij geven jouw persoonsgegevens niet door aan andere bedrijven of instellingen, behalve als wij hiertoe wettelijk verplicht zijn (bijvoorbeeld in geval van belastingaangifte of als de politie dat eist bij een vermoeden van een misdrijf), om de (arbeids-)overeenkomst met jou uit te voeren of als wij daar een gerechtvaardigd of vitaal belang bij hebben. De volgende partijen ontvangen in ieder geval jouw gegevens:

- Pensioenverstrekker
- Salarisadministratiekantoor
- Verzekeringsbedrijf
- Accountant
- Arbodienst
- IT-dienstverlener(s)
- UWV
- Belastingdienst
- Externe adviseurs
- Opleidingsinstanties/externe trainers

Met deze partijen hebben wij waar wettelijk gezien nodig, een verwerkersovereenkomst of data-uitwisselovereenkomst gesloten. In een dergelijke overeenkomst spreken wij met de partijen af wat zij met jouw gegevens mogen doen en dat zij jouw gegevens adequaat moeten beveiligen.

Het kan voorkomen dat de bedrijven of instellingen waaraan we je persoonsgegevens doorgeven, buiten de Europese Economische Ruimte (EER) gevestigd zijn. Wij zorgen ervoor dat wij jouw persoonsgegevens alleen doorgeven aan bedrijven of instellingen buiten de EER als er een passend beschermingsniveau is.

4. Welke rechten heb je?

Elke betrokkene heeft dezelfde privacy rechten. Dus net als onze leerlingen en hun ouders, verzorgers of voogden, heb jij ook als medewerker bepaalde rechten.

4.1 Rechten van betrokkenen

Je kunt gebruik maken van de volgende rechten:

- Recht op **inzage**: het recht om de persoonsgegevens die wij van jou verwerken, in te zien.
- Recht op **rectificatie**: het recht om de persoonsgegevens die wij van jou verwerken, te corrigeren of aan te vullen, bijvoorbeeld indien deze onjuist of onvolledig zijn.
- Recht van **bezwaar**: je kunt in sommige gevallen bezwaar maken tegen de verwerking van je persoonsgegevens.
- Recht op **verwijdering**: je kunt ons verzoeken je persoonsgegevens te verwijderen.
- Recht op **overdraagbaarheid** van gegevens: je hebt het recht om de persoonsgegevens die wij van jou verwerken om de arbeidsovereenkomst uit te voeren te laten overdragen in een digitaal leesbaar standaardformaat naar een derde partij.
- Recht op **beperking** van de verwerking: in sommige gevallen kun je verzoeken om het verwerken van je persoonsgegevens (al dan niet tijdelijk) te beperken wat betekent dat wij minder gegevens van jou verwerken.
- De mogelijkheid om **toestemming in te trekken**, wanneer wij persoonsgegevens verwerken op basis van toestemming.

Wij hanteren in principe een uiterlijke reactietermijn van een maand. Deze termijn kan echter worden verlengd om redenen die verband houden met de complexiteit van het verzoek en het aantal verzoeken. Als wij deze termijn verlengen, stellen wij je daar tijdig van op de hoogte. We kunnen echter niet altijd aan je verzoek voldoen, bijvoorbeeld wanneer je vraagt om verwijdering van je persoonsgegevens en wij van de wet je gegevens nog een aantal jaar moeten bewaren. Daarnaast kan het zo zijn dat wij zwaarwegende belangen hebben om niet (geheel) aan je verzoek te voldoen. Als dat het geval is, informeren wij je daarover.

4.2 Klacht indienen

Als jij vindt dat wij niet op de juiste manier omgaan met jouw persoonsgegevens, dan kun je contact opnemen met onze FG, die verantwoordelijk is om erop toe te zien dat wij de AVG naleven.

Je hebt ook het recht om een klacht in te dienen bij de toezichthouder. Deze heet de Autoriteit Persoonsgegevens.