Stichting
Hervormde scholen
Barneveld, Ede en omstreken

Gedragscode

Geloofwaardig, betrokken en duurzaam

Stichting Hervormde scholen
Barneveld, Ede en omstreken

Contactgegevens
Stichting Hervormde Scholen
Barneveld, Ede en omstreken
Lange Voren 88
3773 AS Barneveld

info@dedrieslag.nl
www.dedrieslag.nl

Datum
23 maart 2020

Status

Ter bespreking/goedkeuring/vaststelling door gremium	datum
Ter bespreking/goedkeuring/vaststelling door gremium	datum

Geloofwaardig, betrokken en duurzaam

Inhoud

1. Algemene afspraken 2
1.1 Inleiding en Werkingsgebied 2
1.2 Algemene normen 2
1.3 Melden van incidenten en datalekken 3

2. Gedragscode 4
2.1 Werkplek 4
2.2 Gegevensdragers 4
2.3 Fysieke informatie 5
2.4 Gebruik eigen apparatuur (BYOD) 5
2.5 Software 6
2.6 Gebruik van e-mail 6
2.7 Gebruik van internet 7
2.8 Gebruik van sociale media 7
2.9 Gebruik beeld- en geluidsmateriaal 8
2.10 Gebruikersnamen, wachtwoorden en pincodes 8
2.11 Delen van informatie 8
2.12 Sleutels 9

3. Controle 10
3.1 Uitgangspunten 10
3.2 Uitvoering van de controle 10

4. Disciplinaire maatregelen 11

1. Algemene afspraken

1.1 Inleiding en Werkingsgebied

Voor een veilig klimaat in de scholen en binnen de kinderopvang is het belangrijk dat de afspraken rondom informatiebeveiliging en privacy door alle werknemers worden nageleefd en uitgedragen. Daarom is deze gedragscode opgesteld waaraan alle medewerkers van onze stichting zich dienen te houden.

Het gebruik van informatie, internet, het (computer)netwerk, en e-mail is voor zowel het personeel als de leerlingen noodzakelijk om het onderwijs goed te kunnen organiseren. Hier kleven echter ook risico's aan. We maken daarom afspraken over de volgende bedrijfsmiddelen:

- Hardware: pc, laptop, tablet, telefoon
- Software (of -systemen): alle applicaties voor het uitvoeren van de werkzaamheden, zoals het leerling volg en administratiesysteem, de e-mailomgeving, en (online)digitaal lesmateriaal maar ook apps op (mobiele) devices.
- Informatie en (persoons)gegevens zowel digitaal als op papier: rapportages, leerling dossiers, gegevens in e-mails, wachtwoorden etc.
- Internetgebruik: het gebruik van e-mail, het bezoeken van websites en gebruik van sociale media.
- Fysieke beveiliging: sleutels, kasten etc.

De afspraken in dit document gelden voor alle locaties van waaruit (school of kinderopvang) werkzaamheden worden verricht (dus ook thuis) en voor alle apparatuur waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij de organisatie maar ook voor uitzendkrachten en tijdelijke werknemers.

1.2 Algemene normen

De volgende algemene normen zijn van toepassing binnen de organisatie.

1. Iedereen heeft een eigen verantwoordelijkheid zorgvuldig om te gaan met persoonsgegevens en (gevoelige) informatie.
2. We spreken elkaar aan als iemand zich niet gedraagt conform deze gedragscode.
3. Sla (persoons)gegevens alleen op de daarvoor ter beschikking gestelde systemen op en sla gegevens altijd op 1 plek op (geen schaduwadministraties opbouwen).
4. We werken binnen de organisatie in principe zo veel als mogelijk digitaal. Dit betekent:
    a. Dat alleen indien dat strikt noodzakelijk is er wordt gewerkt met papieren dossiers.
    b. Informatie die op papier wordt ontvangen wordt gescand en digitaal wordt opgeslagen.
    c. De bron van alle gegevens omtrent leerlingen en ouders/verzorgers is altijd het leerlingvolgsysteem of het kindvolgsysteem.
    d. Personeelsgegevens worden alleen opgeslagen in daarvoor bedoelde systemen. (financiële administratiesysteem en HR systeem)
5. Ouders en medewerkers hebben het recht om hun dossier in te zien. Zorg er daarom voor dat de gegevens zodanig zijn geformuleerd dat dit kan. Het past ook bij je houding als professional.
6. Voer geen vertrouwelijke telefoongesprekken op een plek waar anderen mee kunnen luisteren.
7. Onderling privé contact (direct, via mail of telefoon etc.) tussen personeel en leerlingen is verboden.

1.3 Melden van incidenten en datalekken

Ondanks de afspraken die we maken kan het voorkomen dat je tegen een ICT incident of datalek aanloopt. Zorg ervoor dat je deze altijd meldt op de volgende wijze:

1. Meld ICT incidenten (storing aan printers, laptops, PC, etc) altijd aan je direct leidinggevende.
2. Meld (mogelijke) datalekken altijd via info@dedrieslag.nl

2. Gedragscode

2.1 Werkplek

Op je werkplek bevinden zich vaak en veel persoonsgegevens Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot informatie waartoe zij geen rechten hebben. De volgende aanvullende afspraken gelden:

1. Vergrendel bij het tijdelijk verlaten van de werkplek altijd de pc (windowstoets+L). Het maakt daarbij niet uit voor hoelang je je werkplek verlaat. (Clear screen)
2. Zet je digibord op freeze als je wachtwoorden intoetst of persoonsgegevens in je scherm ziet staan. En zorg dat niemand meekijkt als jij je wachtwoord intoetst. Voordat je het weet zien leerlingen gevoelige gegevens of kunnen ze aan de hand van je afgekeken gebruikersnaam en wachtwoord proberen in te loggen.
3. Zet de notificatie-functie van je e-mail uit, zodat er tijdens je les geen meldingen op het bord binnen komen die leerlingen kunnen zien, maar niet voor hun ogen bestemd zijn.
4. Op alle computers dient een schermbeveiliging te worden ingesteld die automatisch in werking treed na 5 minuten van inactiviteit, hierna dient de computer slechts met een wachtwoord weer geactiveerd te kunnen worden.
5. Laat geen persoonsgegevens of andere vertrouwelijke informatie op je werkplek achter als je afwezig bent. (Clean desk)
6. Sla persoonsgegevens nooit op de lokale schijf (C:) op maar gebruik hiervoor de netwerkschijven of cloud dienst. Dit geldt in het bijzonder ook indien op eigen apparatuur wordt gewerkt.
7. Je accounts voor het netwerk of applicaties zoals het leerlingvolgsysteem zijn altijd persoonlijk, deel deze nooit en laat collega's nooit op jouw account werken.
8. Sluit na gebruik altijd de computer af of log uit.

Indien de school mobiele apparatuur ter beschikking stelt gelden de volgende aanvullende afspraken:

1. Apparatuur mag niet worden meegenomen buiten de school zonder voorafgaande toestemming van de directie.
2. Laat apparatuur nooit onbeheerd achter in auto's of openbare ruimten.
3. Berg mobiele apparatuur altijd achter slot en grendel op als je ze niet gebruikt of na werktijd, zeker tijdens vakantieperiodes. Het is een open deur, maar toch gebeurt het heel erg makkelijk. Maak elkaar er dus op attent als je een laptop of tablet onbeheerd ziet liggen. Als je computer gestolen wordt, heeft dat gevolgen voor de school en de leerling.

2.2 Gegevensdragers

Informatie dient zich altijd binnen een beveiligde omgeving te bevinden. Daarom gelden de volgende afspraken ten aanzien van gegevensdragers:

1. Het gebruik van USB sticks en andere type gegevensdragers (datacards, externe harde schijven) is verboden. Sla onder geen beding persoonsgegevens op externe gegevensdragers op.
2. Indien het met toestemming van de directie toch wordt toegestaan om voor specifieke doeleinden gegevens op te slaan op gegevensdragers dan dienen deze gegevens altijd te worden versleuteld.

2.3 Fysieke informatie

1. Sluit kasten en laden waarin zich persoonsgegevens bevinden altijd af. Het maakt daarbij niet uit voor hoe lang je afwezig bent.
2. Laat nooit sleutels achter in kasten of laden waarin zich persoonsgegevens bevinden.
3. Print altijd beveiligd en laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan.
4. Gebruik postvakjes niet als dossierkast en plaats nooit vertrouwelijke informatie in postvakjes.
5. Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd direct door de papierversnipperaar of laat ze achter in de daarvoor bestemde beveiligde container.
6. Zorg ervoor dat in je klassenmap en lokaal geen persoonsgegevens aanwezig zijn die niet strikt noodzakelijk zijn:
    a. Gebruik waar mogelijk alleen voornamen.
    b. Bewaar adressenlijsten digitaal of achter slot en grendel.
    c. Bewaar medische gegevens digitaal of achter slot en grendel.
    d. Bewaar rapporten en overige informatie over de resultaten van leerlingen digitaal of achter slot en grendel.
    e. Bewaar nooit inloggegevens op papier.
    f. Laat na schooltijd nooit persoonsgegevens in de klas of in de school slingeren. Berg deze na schooltijd altijd achter slot en grendel op.
7. Neem persoonsgegevens nooit mee buiten de school zonder voorafgaande toestemming van de directie.

2.4 Gebruik eigen apparatuur (BYOD)

De afspraken in deze gedragscode hebben betrekking op alle apparatuur. Dus zowel apparatuur die door de organisatie ter beschikking is gesteld maar zeker ook op privé apparaten die worden gebruikt voor je werkzaamheden.
We verwachten dat je in principe apparatuur gebruikt die door de stichting ter beschikking is gesteld en beheerd wordt. Voor eigen apparatuur zoals laptops en telefoons ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Daarom wordt verwacht dat je minimaal de volgende beveiligingsmaatregelen neemt:

1. Eigen apparatuur die wordt gebruikt voor werkzaamheden is altijd voorzien van een eigen account. Deze mag niet gedeeld worden met collega's of huisgenoten.
2. Eigen laptops worden met een wachtwoord beveiligd conform de eisen die gelden voor de apparatuur van de organisatie (zie 2.10-2).
3. Mobiele telefoon en tablets worden altijd voorzien van een schermbeveiliging waarvan het wachtwoord langer is dan 4 tekens.
4. Persoonsgegevens van de organisatie worden nooit op eigen apparatuur opgeslagen.
5. Houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks).
6. Op laptops wordt een virusscanner geïnstalleerd. Dit mag geen gratis software zijn. Zorg ook voor het periodiek (maandelijks) scannen van de apparatuur.
7. Laat apparatuur nooit onbeheerd achter in auto's of openbare ruimten.

2.5 Software

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

1. Het installeren van externe software (van het internet) is uitdrukkelijk verboden zonder toestemming van de ICT afdeling of directie.
2. Installeren van software wordt binnen de organisatie alleen toegestaan met de juiste licenties.
3. Download nooit software van een onbekende bron.

2.6 Gebruik van e-mail

Voor het gebruik van de mailaccounts en mail applicatie die de organisatie ter beschikking stelt gelden de volgende afspraken.

1. Gebruik het e-mail adres alléén voor werk gerelateerde zaken.
2. Gebruik voor privé e-mail een eigen privé e-mailadres (bijvoorbeeld Gmail of Hotmail). Gebruik je privé adres nooit voor communicatie vanuit je professionele rol.
3. Gebruik voor berichten aan meer dan 1 persoon altijd de BCC regel. Zo blijven mailadressen afgeschermd.
4. Het is niet toegestaan om dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en kettingmailbrieven te verzenden of door te sturen;
5. Verzend nooit gevoelige persoonsgegevens via de mail.
6. Indien het noodzakelijk is mails met (bijlagen met) persoonlijke gegevens te verzenden zorg er dan voor dat de bijlagen altijd versleuteld worden.
7. Wees in mails zeer terughoudend met het delen van persoonsgegevens. Als het kan gebruik dan alleen initialen of gebruik geen gegevens die naar een persoon te herleiden zijn.
8. Gebruik je mailbox nooit als opslagplaats voor bijzondere of gevoelige persoonsgegevens.
9. Schoon je mailbox minimaal maandelijks op.
10. Op e-mailberichten is de Wet op het Briefgeheim van toepassing en deze zullen dienovereenkomstig worden behandeld. Het is dan ook niet toegestaan om voor andere gebruikers bestemde email berichten doelbewust ongeautoriseerd te lezen, kopiëren, wijzigen, door te sturen of te vernietigen. Indien sprake blijkt te zijn van een foutief email adres stel de juiste ontvanger of afzender dan direct op de hoogte.
11. Het is niet toegestaan inkomende privé berichten te genereren door deel te nemen aan niet-zakelijke nieuwsgroepen, abonnementen, nieuwsbrieven en dergelijke;
12. Wanneer je een bericht stuurt met belangrijke en/of gevoelige informatie naar (een groep) ouders/verzorgers laat dit dan nalezen door een collega. Een foutje is snel gemaakt en bovendien kan een ander kan je boodschap anders interpreteren dan jij hem bedoeld hebt. Het is dan fijn als er iemand met je meeleest voordat je hem verstuurt.

Medewerkers dienen zich daarnaast bewust te zijn van de gevaren die onzorgvuldig gebruik van internet en E-mail voor de bedrijfsvoering kunnen opleveren. Aanvallen van malware, virussen of andere kwaadaardige programmatuur kan voor de organisatie grote gevolgen hebben. Daarom dien je het volgende in acht te nemen:

13. Klik nooit op onbekende links waarvan de werking of de bron onduidelijk is of die ongevraagd verschijnen.
14. Open nooit mails met twijfelachtige afkomst of “verdachte” bijlagen.
15. Open nooit SPAM berichten.
16. Meld (vermoedelijke) incidenten, inbreuken op de beveiliging en ongewenste of (mogelijk) schadelijke berichten onmiddellijk telefonisch of mondeling bij de ICT afdeling.

2.7 Gebruik van internet

Gebruik van het internet is in principe gebonden aan de werkzaamheden. Privé gebruik is beperkt toegestaan. Gebruik hiervan is verbonden aan de volgende afspraken:

1. Maak alleen gebruik van beveiligde (draadloze) netwerken. Werkzaamheden uitvoeren op onbeveiligde netwerken is verboden.
2. Beperkt persoonlijk gebruik is toegestaan, mits dit
   a. niet storend is voor de dagelijkse werkzaamheden
   b. niet voor commerciële doeleinden is
3. Het is niet toegestaan om
   a. Gegevens van de organisatie op te slaan in openbare cloud omgevingen zoals Dropbox.
   b. Op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten, of dergelijk materiaal te downloaden.
   c. Films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron.
   d. Onder lestijd internettoegang te gebruiken voor privédoeleinden
   e. Deel te nemen aan kansspelen.
   f. 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.
   g. Zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op het internet;
   h. opzettelijk informatie waartoe men via internet toegang heeft verkregen zonder toestemming te veranderen of te vernietigen.
   i. Anoniem of onder een fictieve naam te communiceren

2.8 Gebruik van sociale media

De volgende afspraken gelden voor het gebruik van sociale media

1. Het delen van informatie op sociale media gebeurd altijd op persoonlijke titel. Je blijft altijd persoonlijk verantwoordelijk voor wat je deelt of publiceert. Alleen met voorafgaande toestemming mag informatie namens de organisatie worden gedeeld. Het noemen van de bedrijfsnaam, verwijzingen naar bedrijfsinformatie of het openbaar maken hiervan op sociale media of op fora is dan ook uitdrukkelijk verboden
2. Houd er rekening mee dat je altijd verbonden bent aan de organisatie. Je bent altijd de vertegenwoordiger van de organisatie, ook als je online een privémening verkondigt. Wees daarom voorzichtig met het online uiten van standpunten. Privé-meningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de school en/of het bestuur..
3. Het is voor medewerkers van ons bestuur niet toegestaan standpunten en/of overtuigingen uit te dragen die strijd zijn met de missie en visie van de school.
4. Publiceer nooit vertrouwelijke informatie op sociale media.
5. Publiceer geen beeldmateriaal of informatie van leerlingen of collega's zonder de uitdrukkelijke voorafgaande aantoonbare toestemming. Controleer bij het delen van beeldmateriaal dus altijd of ouders hier toestemming voor hebben gegeven.
6. Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn.
7. Het is medewerkers niet toegestaan om met een privé account 'vrienden' te worden met leerlingen en ouders op sociale media.

8. Inzetten van sociale media in het lesprogramma is gebonden aan de toestemming van ouders als leerlingen jonger zijn dan 16 jaar, het gaat hier om het aanmaken van een (privé)account voor online diensten zoals Pinterest, Canva, Google etc.

2.9 Gebruik beeld- en geluidsmateriaal

Het gebruiken van beeld- en geluidsmateriaal (foto's video's etc.) van leerlingen of collega's mag alleen als daar vooraf uitdrukkelijk toestemming voor is gegeven. Dit geldt voor alle verwerkingen hiervan zowel in de klas, de school als op internet of intranet. Voor leerlingen jonger dan 16 jaar geldt dat de ouders toestemming moeten hebben gegeven. Zonder toestemming is gebruik van beeld of geluidsmateriaal verboden.

2.10 Gebruikersnamen, wachtwoorden en pincodes

Het beveiligen van toegang tot informatie begint met vertrouwelijke inlog gegevens en een sterk wachtwoord. Voor het gebruik van deze gegevens gelden de volgende afspraken:

1. Deel gebruikersnamen en wachtwoorden nooit, ook niet incidenteel. Deze zijn strikt persoonlijk.
2. Wachtwoorden moeten minimaal 8 tekens bevatten, met minstens drie van de volgende vier elementen : kleine letter, hoofdletter, cijfer of speciaal teken (!@#$%^&*()
3. Het wachtwoord mag niet hetzelfde zijn als de inlognaam (of de accountnaam)
4. Schrijf wachtwoorden nooit op. Maak bijvoorbeeld gebruik van wachtwoordkluisjes, zoals Last Pass of True Key
5. Schakel de "automatisch onthouden" functie voor wachtwoorden uit op applicaties/websites waar zich persoonsgegevens bevinden. In het leerlingvolgsysteem mag deze bijvoorbeeld nooit aanstaan.
6. Pincodes (op telefoon of tablet) moeten langer zijn dan 4 tekens.
7. Wachtwoorden moeten elke 3 maanden worden gewijzigd.
8. Gebruik niet voor elke systeem hetzelfde wachtwoord.
9. Voor het leerlingvolgsysteem en andere applicaties waar zich persoonsgegevens bevinden wordt indien mogelijk altijd gebruik gemaakt van twee factor authenticatie.
10. Bij het minste vermoeden van misbruik dient het wachtwoord direct te worden gewijzigd en dient hiervan melding te worden gemaakt.

2.11 Delen van informatie

Het is belangrijk dat we als organisatie zorgvuldig en terughoudend zijn in het delen van informatie. Daarom gelden de volgende afspraken:

1. Voordat je gegevens deelt: Ga na welke afspraken er binnen de school en de kinderopvang gemaakt zijn voordat je persoonsgegevens uitwisselt met derden.
2. Vertrouwelijke gegevens en bedrijfsgevoelige informatie mogen niet zonder toestemming van de directie naar buiten de organisatie worden verstuurd. Als je twijfelt, overleg dan eerst intern.
3. Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist of een arbo- of schoolarts dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en houd daarbij ook rekening met de eventuele verdeling van het ouderlijk gezag
4. Voor de uitwisseling van gegevens met het samenwerkingsverband, Jeugdzorg/CJG of een andere school of kinderopvangorganisatie gelden aparte afspraken. Indien je niet zeker weet of informatie gedeeld mag worden overleg dan met de directie en/of de intern begeleider.
5. Als derden om gegevens vragen controleer dan eerst of deze gegevens wel mogen worden gedeeld. Bij twijfel, overleg dan eerst.

6. Als je informatie met collega's of externen deelt doet dan voor zo ver als mogelijk altijd door het verzenden van een link naar een gedeeld document op het netwerk of een link naar het leerlingvolgsysteem. (b.v in Parnassys of Kindkans)

2.12 Sleutels

Onbeheerde sleutels leiden tot onbeheerde informatie en al snel tot datelekken. Daarom gelden de volgende afspraken:

1. Laat sleutels nooit in deuren of kasten achter.
2. Sluit sleutelkluisjes altijd af.
3. Meld het direct als sleutels zoek raken of worden gestolen.
4. Sleutels zijn persoonlijk. Leen deze niet uit zonder dat je je ervan verzekerd dat deze persoon toegang tot alle informatie mag hebben waar de sleutel toegang toe bied.

3. Controle

3.1 Uitgangspunten

De organisatie kan controle uitvoeren op het naleven van de afspraken uit deze gedragscode. Dit heeft consequenties voor de privacy van het personeel. Deze controle zal dan ook alleen plaatsvinden:

1. In beginsel op basis van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
2. Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode, in opdracht van de directie gerichte controle plaatsvinden. In geval dat ten aanzien van een gebruiker, vanwege een concreet vermoeden van oneigenlijk gebruik, een gerichte controle is uitgevoerd, stelt de directie deze gebruiker(s) daar van zo spoedig mogelijk nadat de controle heeft plaats gevonden op de hoogte.
3. Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van de directie controle op de inhoud plaats.
4. Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken medewerker besproken. De medewerker heeft daarbij altijd de mogelijkheid om dit toe te lichten.
5. E-mailberichten van leden van de GMR onderling, van vertrouwenspersonen, bedrijfsartsen en van een ieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Ook hier kan bij zwaarwegende redenen van afgeweken worden.

3.2 Uitvoering van de controle

1. De controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering.
2. 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.
3. De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens.
4. 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 controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. De organisatie 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. Het bestuur zal mensen met toegang daartoe contractueel verplichten tot afdoende geheimhouding. Daarnaast heeft het personeel recht te weten welke gegevens de organisatie over haar verwerkt in het kader van controle. Daarom heeft het personeel hier alle rechten die de wet aan betrokkenen geeft. (o.a. inzage, correctie en verwijdering).

4. Disciplinaire maatregelen

Bij handelen in strijd met deze regeling of wettelijke bepalingen kunnen afhankelijk van de aard en de ernst van de overtreding maatregelen worden getroffen. Hierbij gaat het om disciplinaire en arbeidsrechtelijke maatregelen zoals berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst of opdracht tot inhuur.
Voordat disciplinaire maatregelen worden getroffen krijgen medewerkers altijd de gelegenheid te reageren op het geconstateerde. Disciplinaire maatregelen kunnen niet enkel op basis geautomatiseerde besluitvorming worden genomen, zoals een constatering van een automatisch filter of blokkade.