Stichting Openbaar Onderwijs Emmen

Gedragscode Veilig gebruik van ICT-middelen

Conform de Algemene Verordening Gegevensbescherming

Versie: 1.2
Vastgesteld GMR: 1 oktober 2020
Vastgesteld bestuur: 6 juli 2023

Bron
Kennisnet

Bewerkt door:
Stichting Openbaar Onderwijs Emmen, A. Sueters

Versiebeheer:

Versie	Status	Datum	Naam
1.0	Definitief	Oktober 2020	A. Sueters
1.1	Concept	Februari 2023	A. Sueters
1.2	Definitief	Juni 2023	A. Sueters

Bijgewerkt:

Datum	Naam	Functie	Aanpassing
JUni 2023	A. Sueters	Privacy Officer	Aanpassingen ICT-leverancier, gebruik prive mail, toevoeging i.v.m. gebruik streaming diensten, toevoeging Zivver, evaluatie een keer in 2 jaar.

Inhoudsopgave

1 Inleiding

Het gebruik van internet, computernetwerk en e-mail is voor alle medewerkers van de school 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 **ICT-middelen** genoemd.
Onder ICT-middelen worden in ieder geval verstaan:

- Hardware: *pc, laptop, tablet, telefoon, hardware token (tag)*.
- 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) devices.*
- Informatie en (persoons)gegevens: *rapportages, leerling dossiers, 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 diensten als FTP en maar ook sociale media zoals Facebook, LinkedIn, Instagram en Twitter.*

Aan het gebruik van deze ICT-middelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van alle medewerkers van het Stichting Openbaar Onderwijs Emmen (verder genoemd: Stichting OOE) wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde ICT-middelen. 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 devices waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij Stichting OOE, ook voor uitzendkrachten en tijdelijke werknemers.

1.1 Uitgangspunten gedragscode

Deze gedragscode legt vast wat er van de medewerkers verwacht wordt met betrekking tot het gebruik van de ter beschikking gestelde ICT-middelen en de inzet van eigen devices voor schoolwerkzaamheden.
Deze gedragscode legt regels vast voor het gebruik van de ICT-middelen 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 privacygevoelige informatie waaronder persoonsgegevens van het schoolbestuur, haar medewerkers, leerlingen en hun ouders/ verzorgers 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/ verzorgers;
- het voorkomen en tegengaan van misbruik van de ICT-middelen;
- 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 ICT-middelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. Stichting OOE 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 en veilig gebruik van ICT-middelen 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.

1.2 Eigen verantwoordelijkheid en privégebruik

Het gebruik van door Stichting OOE verstrekte ICT-middelen is persoonlijk (voor eigen gebruik) en blijft de verantwoordelijkheid van de medewerker. Alle devices die voor schoolwerk worden gebruikt (inclusief eigen devices) worden niet uitgeleend of aan anderen ter beschikking gesteld zonder aanvullende (beveiliging)maatregelen. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen.

1.3 Verschillende soorten gegevens

Stichting OOE is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en is het beschermen van gegevens.
Stichting OOE 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 Stichting OOE bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- **Vertrouwelijke gegevens**: dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen Stichting OOE toegankelijk zijn. Denk hierbij aan (bijzondere) persoonsgegevens, personeelsgegevens of aanbestedingsgegevens.

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

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

2 Gedragscode

In deze gedragscode voor veilig gebruik van ICT-middelen geeft Stichting OOE aan wat de afspraken zijn met betrekking tot verschillende onderwerpen rondom het gebruik van ICT-middelen 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 zoals genoemd in het Informatiebeveiligings- en privacy beleid 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 ICT-middelen. (beveiligingsmaatregelen).

- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild.
- Meld diefstal of verlies van ICT-middelen onmiddellijk na constatering door het sturen van een e-mail aan ICT-adviseur en Privacy Officer . Zie voor nadere informatie Protocol Informatiebeveiligingsincidenten en datalekken.

2.2 Computergebruik

Voor het uitoefenen van de werkzaamheden stelt Stichting OOE aan de medewerker computer- en netwerkfaciliteiten (ICT-middelen) ter beschikking. Het gebruik van deze ICT-middelen 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-middelen 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 Stichting OOE, 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 ICT-leverancier volgens interne afspraken.

2.3 Werkplek

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot ICT-middelen 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 clear screen regels:

- Vergrendel bij het tijdelijk verlaten van de werkplek de pc (windowstoets + L).
- Verwijder interne en vertrouwelijke documenten 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.

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 het Protocol Beveiligingsincidenten en Datalekken van Stichting OOE.

2.4 Gebruik eigen devices (BYOD)

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor Stichting OOE worden uitgevoerd. Stichting OOE is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de ICT-middelen van de school.

Voor ‘Own Devices’ (eigen devices: bijvoorbeeld eigen telefoon of laptop) ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de

medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

- Beveilig het device met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode die langer is dan 4 tekens.
- Vergrendel het device bij het verlaten van de werkplek (windowstoets + L).
- Sla persoonsgegevens van medewerkers, leerlingen en externen niet op het eigen device; **dit is niet toegestaan.**
- Beveilig alle gegevens, anders dan persoonsgegevens, met betrekking tot Stichting OOE als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden (denk hierbij aan het eigen device of usb-stick).
- Scheid gegevens, anders dan persoonsgegevens, van Stichting OOE en privégegevens van elkaar.
- 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.

Stichting OOE mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van Stichting OOE 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 Stichting OOE. 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 Stichting OOE alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen.
- Bij het gebruik van onlinesoftware, app's 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 Stichting OOE persoonsgegevens verwerkt. Regel dit vooraf aan het gebruik.
- Aanvragen van digitaal lesmateriaal en/of andere software volgt bij Stichting OOE de afgesproken aanvraagprocedure. Hiervoor is een aanvraagformulier beschikbaar wat als uitgangspunt dient voor eventuele wettelijk verplichte aanvullende privacy- en/of beveiligingsmaatregelen (document in concept).

2.6 Gebruik van e-mail

Stichting OOE 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.
- Wanneer persoonsgegevens via de mail worden gedeeld, maak je gebruik van Zivver.
- Ontvangen en versturen van privémail op het school e-mailadres is incidenteel toegestaan, mits dit niet in strijd is met belangen van OOE.
- 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 devices (tablet, telefoon) dan kan Stichting OOE, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het device gewist worden.

2.7 Gebruik van internet

Stichting OOE 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
  - op internetsites 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;
  - streaming diensten door middel van prive accounts te gebruiken binnen de organisatie;
  - 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 devices gebruikt. Menselijk (online)handelen staat veelal aan de basis van een datalek.
Stichting OOE 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 Stichting OOE;
- 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 Stichting OOE netwerk is 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 social 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 gebruik van social media geldt als uitgangspunt dat het digitale gedrag op social media niet afwijkt van het real life gedrag binnen de school. Medewerkers zijn altijd de vertegenwoordiger van Stichting OOE ook als zij online een privémening verkondigen.
Bij Stichting OOE gelden de volgende afspraken voor het gebruik van social media:

- Deel op verantwoorde wijze kennis via social media rekening houdend met de goede naam van Stichting OOE en iedereen die hierbij betrokken is.
- Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens Stichting OOE gedaan wordt.
- Publiceer geen vertrouwelijke informatie op sociale media.
- Publiceer geen beeldmateriaal van leerlingen zonder de uitdrukkelijke voorafgaande aantoonbare toestemming van ouders/ verzorgers als de leerling jonger is dan 16 jaar of van de leerling zelf als deze ouder is dan 16 jaar.
- 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 Stichting OOE.

Aanvullende afspraken rondom social media in het algemeen zijn vastgelegd in een Sociale Media Protocol (voor medewerkers) binnen Stichting Openbaar Onderwijs Emmen.

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 Stichting OOE mag alleen als daar vooraf toestemming voor gegeven is door ouders/ verzorgers 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.

- Het Stichting OOE verwijst hierbij naar de richtlijn die is opgesteld voor het gebruik en toestemming van beeldmateriaal.
- 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 devices (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 minimaal 8 tekens bevatten, met minstens drie van de volgende vier elementen: kleine letter, hoofdletter, cijfer of speciaal teken (&, ?, #, !, %, enz.).
- Gebruik wachtzinnen van minimaal 4 woorden, om het wachtwoord makkelijker te onthouden. *Bijvoorbeeld: 100KilometerPerUurIsTeLangzaam@.*
- Het wachtwoord mag geen makkelijk te raden persoonlijke informatie bevatten, zoals een naam, geboortedatum of adres.
- Pincodes (op telefoon of tablet) moeten langer zijn dan 4 tekens.
- Wachtwoorden moeten volgens de afspraken binnen Stichting OOE op aangegeven tijden vervangen worden.
- Gebruik niet voor elke 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 het Protocol Informatiebeveiligingsincidenten en datalekken van Stichting OOE.

3 Controle gebruik ICT-middelen

Stichting OOE handelt bij de controle op het gebruik van ICT-middelen binnen de geldende wet- en regelgeving, te weten:

- De Grondwet,
- Algemene Verordening Gegevensbescherming (AVG)
- Wet Medezeggenschap Onderwijs (WMO)
- Burgerlijk Wetboek (BW)
- Wetboek van Strafrecht
- Cao PO en
- Cao VO.

Stichting OOE zal bij controle rondom het gebruik van ICT-middelen op basis van deze gedragscode uitgaan van de juiste balans tussen verantwoord gebruik van ICT-middelen en de bescherming van de privacy van medewerkers.

3.1 Voorwaarden voor controle

- Controle van persoonsgegevens met betrekking tot gebruik van ICT-middelen 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 Stichting OOE gerichte controle plaatsvinden.
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van Stichting OOE, 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 met de betrokken medewerker besproken. Stichting OOE 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.

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, 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 Stichting OOE worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- Door Stichting OOE 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 schoolbestuur van Stichting OOE, 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. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens worden getroffen, zoals een constatering van een automatisch filter of blokkade. 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 (G)MR

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle van het gedrag of de prestaties van medewerkers. Het medezeggenschapsorgaan (de GMR) is om deze reden instemming plichtig. De GMR heeft op 1 oktober 2020 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 tweejaarlijks geëvalueerd door stichting OOE.