Gedragscode informatiebeveiliging

Samenwerkingsverband
Primair Onderwijs Zaanstreek

Versie	Status	Datum	Naam	Omschrijving
2.0	CONCEPT	14-5-2018	Bernard Homans	
2.0	Vastgesteld	29-5-2018	Bestuur SWV	
2.1	CONCEPT	30-3-2023	Karina Knaap	
2.2	Concept	21-5-2024	Karina Knaap	

Inhoudsopgave

1 Inleiding

Het samenwerkingsverband heeft geen personeel rechtstreeks in dienst. Medewerkers die werkzaamheden voor de organisatie van het samenwerkingsverband uitvoeren, zijn of ingehuurd of in dienst van aangesloten besturen. Daar waar 'medewerker' staat, wordt altijd bedoeld de medewerker die werkzaamheden voor het samenwerkingsverband uitvoert, ongeacht bij deze in dienst is. Deze medewerkers zijn dagelijks betrokken bij het uitvoeren van taken van en het samenwerkingsverband. Daardoor komen zij dagelijks in aanraking met informatie over leerlingen en privacygegevens van schoolpersoneel, bestuurders en personeel van de besturenorganisaties. Deze informatie moeten we vertrouwelijk behandelen. Het samenwerkingsverband is gehouden een hoog beveiligingsniveau te garanderen, zodat scholen, schoolbesturen en ketenpartners hun informatie met een gerust hart met ons kunnen delen.

Het gebruik van internet, computernetwerk en e-mail is noodzakelijk voor alle medewerkers die werkzaamheden verrichten voor het samenwerkingsverband 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 enz..*
- Software (of -systemen): *alle applicaties voor het uitvoeren van de werkzaamheden, zoals de bedrijfs-emailomgeving, Microsoft Office, administratiesystemen, maar ook apps op (mobiele) devices, enz..*
- Informatie en (persoons)gegevens: *rapportages, personeelsdossiers, gegevens in e-mails, enz.. Hierbij vraagt de verwerking van persoonsgegevens vanuit de privacywetgeving extra maatregelen.*
- Internetgebruik: *het bezoeken van het World Wide Web, het gebruik van e-mail , maar ook sociale media zoals Facebook, LinkedIn, Instagram, tiktok en Twitter enz..*

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers die werkzaamheden voor het samenwerkingsverband verrichten wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen met het oog op het omgaan met privacygegevens. Dit wordt verwacht van medewerkers bij het gebruik van bedrijfsmiddelen om werkzaamheden voor het samenwerkingsverband uit te voeren, of het nu om middelen gaat die hen door hun directe werkgever ter beschikking zijn gesteld, door het samenwerkingsverband of bij gebruik van eigen middelen.

De afspraken in dit document gelden voor alle locaties van waaruit werkzaamheden worden verricht en voor alle devices waarmee werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam verricht voor het samenwerkingsverband.

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, dit alles met het oog op het omgaan met privacygegevens. Het doel van deze gedragscode is om de normen en uitgangspunten vast te leggen ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen misbruik
-

- de bescherming van privacy gevoelige informatie waaronder persoonsgegevens van leerlingen en hun ouders en van medewerkers die werkzaamheden verrichten voor het samenwerkingsverbanden en daarmee het beschermen van de privacy en veiligheid van alle betrokkenen
- de bescherming van vertrouwelijke informatie binnen het samenwerkingsverbanden en van medewerkers
- het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen

Het samenwerkingsverband zal de controle en handhaving uitvoeren van deze regels conform de privacywetgeving en het algemene arbeidsrechtelijk kader.

1.2 Eigen verantwoordelijkheid en privégebruik

Het gebruik van door het samenwerkingsverband verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle devices die voor het werk worden gebruikt (inclusief eigen devices '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.

Het samenwerkingsverband is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens. Het samenwerkingsverband 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 het samenwerkingsverband bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- **Vertrouwelijke gegevens**; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen het samenwerkingsverband 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, allen die in de gremia en werkgroepen van het samenwerkingsverband een rol spelen, als relaties.

1.3 Privacywetgeving

De privacywetgeving verplicht elk individu om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat het samenwerkingsverband schriftelijk afspraken maken met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk). Deze afspraken worden vastgelegd in een Verwerkersovereenkomst.
Conform de privacywetgeving heeft het samenwerkingsverband een Functionaris voor gegevensbescherming aangesteld (FGB). Voor het samenwerkingsverband is dat degene die in het IBP wordt genoemd. Deze communiceert intern over en controleert de uitvoering van de gedragsregels die horen bij het verwerken van persoonsgegevens.

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 mogelijk een datalek

kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en Het samenwerkingsverband.
Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt het samenwerkingsverband 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 het samenwerkingsverband goedgekeurde bedrijfsmiddelen.

Van medewerkers die werkzaamheden voor het samenwerkingsverbanden verrichten/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bv. leerlingdossiers, vertrouwelijke enquêtegegevens, gegevens van medewerkers et cetera, wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. 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 betrokkene of leidinggevende te gebruiken en/of naar buiten te brengen.

2 Gedragscode

In deze gedragscode voor informatiebeveiliging geeft het samenwerkingsverband als volgt nader aan wat de afspraken zijn met betrekking tot die informatiebeveiliging 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’:

- Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht[1].
- Voorkom het lekken van interne en vertrouwelijke informatie.
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen. (beveiligingsmaatregelen).
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild (bijvoorbeeld door jailbreaks[2]).
- Voorkom diefstal of verlies van bedrijfsmiddelen en meld onmiddellijk na constatering hiervan door het sturen van een e-mail aan - of het telefonisch melden bij - de daarvoor aangewezen persoon. Zie hiervoor de procedure meldplicht datalekken van het samenwerkingsverband, paragraaf 2.13.

[1] Basisregels: persoonsgegevens mogen niet verspreid worden zonder toestemming van de persoon. Gegevens mogen niet worden gearchiveerd worden zonder toestemming tenzij daar wettelijk uitzonderingen voor gelden. Bijzondere persoonsgegevens vragen om extra bescherming.
[2] Jailbreak (letterlijk: (gevangenis)uitbraak) is een Engelse term voor de handeling die het mogelijk maakt om op een iPhone, iPod touch, iPad en Apple TVsoftwaretoepassingen te laden die door de firma Apple niet erkend zijn. Voor meer info klik hier.

2.2 Toegangsbeveiliging gebouw

- Sleutels en toegangscodes zijn persoonlijk. Wissel ze nooit onderling uit en ook niet met huisgenoten.

2.3 Bezoekers

- Bezoekers wachten bij de receptie van de organisatie waar hij/zij op dat moment werkt. De medewerker haalt zijn bezoek(ers) zelf op bij de receptie. Of de receptiemedewerker brengt de bezoeker naar de medewerker.
- De medewerker is zelf verantwoordelijk voor de bezoeker tijdens het bezoek.
- De bezoeker wordt door de medewerker zelf uitgeleide gedaan.

2.4 Computergebruik

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor het samenwerkingsverband worden uitgevoerd. Medewerkers zijn zelf verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen. Hiervoor gelden de volgende afspraken:

- Beveilig het device met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode van minstens 4 tekens.
- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden, zoals collega's, medebewoners, familieleden en bezoekers.
- Stel de e-mailapp op de mobiele telefoon zo in dat er geen leesbare pop-ups verschijnen.
- 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 werkzaamheden.
- Sla persoonsgegevens alleen op de daarvoor aangewezen systemen op. (Opslaan van deze gegevens in public Cloud omgevingen, zoals een persoonlijke Dropbox, is niet toegestaan).
- Persoonsgegevens, opgeslagen op mobiele datadragers zoals laptop, usb-stick, of harddisc dienen versleuteld te zijn.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Sluit na gebruik de computer af of log uit.
- Gegevensdragers of apparaten die worden vervoerd van of naar de klantlocatie en klantinformatie bevatten worden niet onbeheerd achtergelaten in de auto.
- Meld storingen van beheerde werkplekken (computer of laptop) bij de ICT-afdeling van je werkgever en bij de daartoe aangewezen persoon bij het samenwerkingsverband.
- Bij de overdracht per e-mail van persoonsgegevens buiten het netwerk is het gebruik van ZIVVER verplicht.

Voor 'Own Devices' ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat de volgende beveiligingsmaatregelen extra worden genomen indien de 'Own Devices' voor het werk worden gebruikt:

- Scheid (versleutelde)gegevens, anders dan persoonsgegevens, van het samenwerkingsverband en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen device.
- 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.

Het samenwerkingsverband mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van het samenwerkingsverband moet de medewerker zelf aantonen dat de bovenstaande maatregelen worden toegepast.

2.5 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 gelden 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).
- Doe kasten met privacygevoelige gegevens op slot bij het verlaten van je werkplek.
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via een beamer) mee kan kijken. Sluit het e-mail programma af en zorg voor een opgeruimd digitaal bureaublad.
- Laat geen afdrukken bij de printer liggen of op je werkplek, zeker niet als er persoonsgegevens op staan.
- Gooi overbodig geworden papieren documenten met persoonsgegevens altijd weg in een papierversnipperaar.
- Laat geen digitale gegevensdragers zoals USB Stick/harddisc en dergelijke onbeheerd achter.

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 meldplicht datalekken van Het samenwerkingsverband, zie paragraaf 2.13.

De in deze paragraaf genoemde punten gelden voor elke werkplek waar je werkzaamheden voor samenwerkingsverband uitvoert.

2.6 Software

De onderstaande regels gelden voor installatie en gebruik van software:

- Installeren van software voor werkzaamheden voor het samenwerkingsverband is alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen.
- Bij het gebruik van online software of app's, wordt gekeken of er persoonsgegevens bij verwerkt worden.
- Een verwerkersovereenkomst wordt afgesloten met elke leverancier van (online)software, die in opdracht van het samenwerkingsverband persoonsgegevens verwerkt. Regel dit vooraf aan het gebruik.

2.7 Gebruik van e-mail

Het samenwerkingsverband 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 bedrijfse-mail adres ***alléén*** voor werk 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).

- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie, zoals correct taalgebruik.
- Synchroniseert een medewerker de bedrijfsemail met een door het bedrijf beschikbaar gestelde devices of een eigen device (tablet, telefoon) dan kan het samenwerkingsverband, 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.
- Privacygevoelige informatie, accountgegevens, wachtwoorden en/of bedrijfsgevoelige gegevens mogen niet onbeveiligd via e-mail verstuurd worden, maar alleen via ZIVVER.

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.
Het samenwerkingsverband verwacht van medewerkers dat zij:

- het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken in internetcafés of hotels) en websites
- geen gebruik maken van een apparaat in een internetcafé of een computer in een hotel voor het inloggen op het netwerk van het samenwerkingsverband
- 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 samenwerkingsverband netwerk is, eigen hotspot of het eigen draadloze netwerk thuis is)
- inloggen op het netwerk van het samenwerkingsverband alleen met een (eigen) beveiligd apparaat.
- bij het verwerken van persoonsgegevens alléén gebruik maken van bekende én beveiligde draadloze netwerken
- weten wat malware is [3], het kunnen herkennen en weten hoe te handelen.

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.
Bij het samenwerkingsverband gelden de volgende afspraken voor het gebruik van sociale media:

- Publiceer geen persoonsgegevens van anderen op sociale media.
- Zonder toestemming mag geen foto van collega's op social media worden geplaatst.

2.10 Gebruik beeld- en geluidsmateriaal

Het gebruiken van beeld- en geluidsmateriaal, het delen van foto's, video's en geluidsfragmenten waarop of waarin medewerkers die werkzaamheden voor het samenwerkingsverband voorkomen,

[3] **Malware** is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Het woord is een samentrekking van het Engelse *malicious software* (kwaadaardige software, soms schadelijke software). (Bron)

mag alleen als daar vooraf toestemming voor is gegeven door betrokkene. Zonder deze toestemming mogen geen foto's, video's en geluidsfragmenten van medewerkers worden gebruikt.

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 (!@#$%^&*()
- Pincodes (op telefoon of tablet) moeten minstens 4 tekens zijn.
- Wachtwoorden moeten volgens de afspraken binnen het samenwerkingsverband op aangegeven tijden vervangen worden (minimaal om de 180 dagen). Het nieuwe wachtwoord mag niet lijken op het laatst gebruikte, dus geen Welkom13, na Welkom12.
- Gebruik niet voor elk systeem hetzelfde wachtwoord.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Wachtwoorden alleen beveiligd opslaan.

2.12 Omgaan met ontvangen gegevens

Persoonsgegevens die voor verwerking aan een medewerker die werkzaamheden voor het samenwerkingsverband verricht, onbeveiligd door derden per e-mail wordt aangeleverd moeten worden geweigerd. De medewerker stuurt de afzender een standaardbericht en vernietigt deze gegevens[4].
Persoonsgegevens die wel beveiligd worden ontvangen maar waarbij met de afzender geen verwerkersovereenkomst is afgesloten moeten ook worden geweigerd. De medewerker stuurt de afzender een standaardbericht en vernietigt deze gegevens.

2.13 Meldplicht Datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens de procedure meldplicht datalekken van het samenwerkingsverband, zie hoofdstuk 4.

3 Controle gebruik bedrijfsmiddelen

Het samenwerkingsverband handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten de Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018).

3.1 Voorwaarden voor controle

- Controle van de beveiliging van persoonsgegevens vindt slechts plaats in het kader van de handhaving 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 die werkzaamheden voor het samenwerkingsverband gerichte controle plaatsvinden.
-

[4] Hiervoor wordt een standaard template opgesteld.

-
-
- Bij constatering van het niet naleven van de gedragscode informatiebeveiliging wordt dit onmiddellijk met de betrokken medewerker besproken. Het samenwerkingsverband zal de medewerker op verzoek inzage verschaffen in de gegevens waarover het samenwerkingsverband beschikt op grond waarvan het niet naleven van de gedragscode is geconstateerd. De medewerker wordt gewezen op de consequenties wanneer de gedragscode niet wordt nageleefd.
- E-mailberichten van leden van de ondernemingsraad 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. Dit geldt niet voor veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.

3.2 Uitvoering van de controle

- 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 op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.
- Betrokken ICT-personeel, 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.

3.3 Disciplinaire maatregelen

Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het bestuur van het samenwerkingsverband, 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, op non-actief stellen en / of beëindiging van de overeenkomst op grond waarvan de medewerker werkzaamheden voor het samenwerkingsverband verricht.
Medewerkers die zich niet aan deze gedragscode houden, worden zo spoedig mogelijk door het bestuur 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/haar zienswijze naar voren te brengen.

4 Procedure meldplicht

- Iedere medewerker heeft de plicht om beveiligingsincidenten en mogelijke datalekken te melden als hij iets verdachts opmerkt. Dit moet worden gemeld middels het versturen van een e-mail naar de FGB, zoals vermeld in het IBP.
- Alle beveiligingsincidenten worden door de FGB geregistreerd.
- Ook wanneer een medewerker denkt dat iets beter kan, kan dat worden gemeld. Dit kan worden besproken met de leidinggevende.

5 Medezeggenschap

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle van het gedrag of de prestaties van medewerkers. Aangezien medewerkers niet rechtstreeks in dienst zijn, is deze gedragscode vanaf inwerkingtreding verbonden aan de overeenkomst met de werkgever van elke medewerker.

6 Definitie persoonsgegevens

Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn.
Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd.

7 Slotbepaling

Deze regeling wordt jaarlijks geëvalueerd door Het samenwerkingsverband met haar medewerkers. De eerstkomende evaluatie vindt plaats in september 2023.

Naam medewerker: ……

Zaanstad, datum: ……

Verklaart de kennis genomen te hebben van de gedragscode en te tekenen voor akkoord.