



Gedragscode



Samen voor mooie en
duurzame provincies

Inhoudsopgave

Gedragscode	2
Natuur en Milieufederatie Flevoland	2
Integriteit.....	2
1. Algemeen.....	2
2. Gedrag.....	3
3. Wetten en regels	4
Databeveiliging.....	4
1. Wees zorgvuldig met alle informatie waarmee je in aanraking komt.....	4
2. Verstrek geen vertrouwelijke gegevens aan derden.....	5
3. Ga zorgvuldig om met ICT-voorzieningen, voorkom ongeautoriseerde toegang.....	5
4. Gebruik internet, e-mail en social media met je volle verstand.....	5
5. Meld datalekken.....	7
6. Spreek collega's aan op onveilig gedrag.....	7
7. Geef je mening over hoe gegevensbescherming veiliger kan.....	7
8. Extra aandachtspunten (met name voor Secretariaat / Marketing / Communicatie).....	7
Overtredingen en sancties	8
Handtekening	10

Gedragcode

Natuur en Milieufederatie Flevoland

Deze gedragscode geldt als gedragsnorm en is van toepassing op zowel de medewerkers (met inbegrip van extern ingehuurd medewerkers/zzp'er, vrijwilligers en stagiairs) en de directeur/bestuurder. De directeur en de bestuurder van Natuur en Milieufederatie Flevoland ondertekenen een integriteitsverklaring. Waar NMFF genoemd staat in deze gedragscode, wordt bedoeld Natuur en Milieufederatie Flevoland

Integriteit

1. Algemeen

- 1.1 Scheid privé en zaken – Zorg dat privéleven en zakelijk leven zich niet vermengen. Om onafhankelijk en oprecht te kunnen handelen, mogen zakelijke beslissingen geen invloed hebben op je privéleven en omgekeerd.
- 1.2 Ga zorgvuldig om met geschenken en giften – Relatiegeschenken worden uitgewisseld om de goede verstandhouding te verstevigen. De schijn moet altijd worden vermeden dat ze als tegenprestatie voor een bepaalde dienst worden gezien. Een geschenk mag dan ook nooit de onafhankelijkheid of de vrijheid van de ontvanger aantasten. Gelet hierop mogen in ieder geval cheques, geld, kostenvergoedingen et cetera niet aangeboden of aangenomen worden. Relatiegeschenken moeten binnen redelijke grenzen blijven: of ze nu worden gegeven of ontvangen. Geschenken met een tegenwaarde van meer dan €50.- mogen niet geaccepteerd, noch gegeven worden.
- 1.3 Privégebruik van NMFF-eigendommen, telefoon, internet en e-mail – Incidenteel en beperkt gebruik van e-mail en internet voor persoonlijke doeleinden is toegestaan, indien dit geen belemmering vormt voor het zakelijke gebruik, niet in strijd is met de NMFF-code dan wel als oneigenlijk gebruik dient te worden beschouwd. Zet professionele hulpmiddelen zoals beamers en kopieerapparaat alleen privé in met toestemming van de directeur.
- 1.4 Houd een deugdelijke administratie bij – vermijd onduidelijke afspraken. Houd er rekening mee dat derden jouw dossiers en administratie (inclusief projectoverzichten, archivering) moeten kunnen begrijpen en dat alle transacties logisch en herleidbaar zijn. Financiële transacties lopen altijd via de directeur. De directeur legt verantwoording af aan de Raad van Toezicht.

- 1.5 Maak duidelijke afspraken met partijen waar je mee samenwerkt – Zorg dat afspraken met partijen duidelijk zijn, zowel voor de NMFF als voor de wederpartij. Voer afspraken pas uit als je zeker weet dat die duidelijkheid er is. Zo voorkom je problemen in de toekomst.
- 1.6 Leg afspraken en wijzigingen schriftelijk vast – Zorg ervoor dat partijen, los van personen, ook na verloop van tijd precies weten wat er is afgesproken.

2. Gedrag

- 2.1 Omgangsvormen – De **NMFF** heeft een informele bedrijfscultuur en de bedrijfsvoering kenmerkt zich door korte lijnen. In de omgang met elkaar nemen we een aantal basiswaarden in acht:
 - behandel elkaar met respect en eerlijkheid
 - werk samen in openheid en vertrouwen
 - ontwikkel jezelf voortdurend
 - neem je voor uitstekend resultaten in je werk te behalen.Deze waarden zijn van toepassing op alle intermenselijke relaties op het werk en in de maatschappij.
- 2.2 Realiseer je wat een ander van je gedrag zou vinden – Raadpleeg de directeur bij twijfel bij het toepassen van deze bepalingen. Is een bepaalde handeling wel of niet toelaatbaar? Het kan je helpen wanneer je je in een dergelijk geval afvraagt wat een collega van je gedrag zou denken.
- 2.3 Besef dat je gedrag op enige wijze de goede naam van de **NMFF** kan aantasten. Onthoud je van gedrag dat de goede naam van de **NMFF** aantast of kan aantasten. Denk na over de consequenties voor de **NMFF** als je handeling bij een groter publiek bekend wordt, bijvoorbeeld via krant of radio. Raadpleeg bij twijfel vooraf de directeur of de communicatiemedewerker.
- 2.4 Seksuele intimidatie is binnen de **NMFF** niet toegestaan. Onder seksuele intimidatie wordt verstaan:
 - Het maken van seksuele toespelingen
 - Handtastelijkheden
 - (Open)Trekken van/aan kleding
 - Het maken van seksuele toespelingen in schriftelijke vorm via brieven, e-mail, stalking en dergelijkeMocht je desondanks in aanraking komen met seksuele intimidatie binnen de organisatie, meld dit dan direct bij de vertrouwenspersoon.

- 2.5 Discriminatie, pesten en ander ongewenst gedrag op welk niveau dan ook, wordt niet geaccepteerd. Is er sprake van discriminatie, pesten of ander ongewenst gedrag, meld dit dan bij de vertrouwenspersoon.

3. Wetten en regels

- 3.1 Handel niet in strijd met wetten en regelgeving - Onthoud je bij de uitvoering van je functie te allen tijde van handelingen die direct of indirect tot gevolg hebben dat jij of de NMFF handelt in strijd met wetten en regelgeving.

Databeveiliging

In beginsel komt het er op neer dat de NMFF's geen mensen benaderen op een manier die niet mag, dat persoonsgegevens niet aan derden worden verstrekt zonder dat de 'klant' dat weet en dat het gebruik van persoonsgegevens op een veilige manier gebeurt. Wees dus 'security aware' als je met persoonsgegevens werkt.

1. Wees zorgvuldig met alle informatie waarmee je in aanraking komt

- 1.1 Ga zorgvuldig om met persoonsgegevens, registreer persoonsgegevens in SPITS Online in plaats van in losse word- en excelbestanden.
- 1.2 Gooi brieven met NAWTE gegevens (naam, adres, woonplaats, telefoonnummer, e-mailadres) of andere persoonsgegevens niet in de oud papierbak, maar versnipper deze.
- 1.3 Als iemand aangeeft dat de NMFF hem niet meer mag bellen, e-mailen of post toesturen, dan zijn wij verplicht om dat direct vast te leggen en daar naar te handelen. Geef dit dus door aan je secretariaat.
- 1.4 Als je een (Excel)bestand met veel persoonsgegevens moet versturen, doe het dan beveiligd met een wachtwoord en stuur het wachtwoord separaat of bel het door.
- 1.5 Neem je persoonsgegevens mee op bijvoorbeeld een USB-stick, laptop of DVD? Zorg er dan voor dat deze informatie beveiligd is.
- 1.6 Gebruik niet je privé-telefoon of laptop om persoonsgegevens van relaties van de NMFF's op te slaan. Mocht dit toch nodig zijn, zorg dan dat anderen er niet bij kunnen. Neem bij voorkeur deze informatie in SPITS Online op en verwijder de informatie van je eigen telefoon of tablet.

2. Verstrek geen vertrouwelijke gegevens aan derden

- 2.1 Verstrek geen persoonsgegevens van relaties aan derden die daar geen recht op hebben.
- 2.2 Het onderling uitwisselen van persoonsgegevens (bijvoorbeeld in vrijwilligersgroepen) is alleen toegestaan met toestemming van de personen die het betreft

3. Ga zorgvuldig om met ICT-voorzieningen, voorkom ongeautoriseerde toegang

- 3.1 Vergrendel je pc (Ctrl + Alt + Delete) als je je werkplek verlaat of sluit je PC af.
- 3.2 Kies veilige wachtwoorden.
- 3.3 Bewaar wachtwoorden op een veilige plaats (zoals een wachtwoordenkluis-programma).
- 3.4 Wijzig je wachtwoorden regelmatig.
- 3.5 Laat geen papieren met persoonsgegevens onbeheerd (op je bureau) achter.
- 3.6 Leen je persoonlijke gebruikersnaam of wachtwoord niet uit, je bent altijd zelf verantwoordelijk voor het gebruik van je account en de daarbinnen uitgevoerde acties.
- 3.7 Zet geen gevoelige persoonsgegevens (zoals een kopie paspoort of personeelsdossier) in een onbeveiligde map. Zorg ervoor dat alleen bevoegden toegang tot deze informatie (op de server) kunnen hebben.
- 3.8 Installeer geen soft- of hardware op je zakelijke devices.
- 3.9 Als je je eigen ICT-middelen (bijvoorbeeld je telefoon, tablet, laptop of PC) gebruikt om toegang te krijgen tot informatie van de NMFF's zorg er dan voor dat deze goed beveiligd zijn.

4. Gebruik internet, e-mail en social media met je volle verstand

- 4.1 Als je een e-mailing verstuurt naar meerdere personen (bulkmail), zet de e-mailadressen dan in de BCC en niet in de CC en richt de mail aan jezelf.
- 4.2 Als je een e-mail doorstuurt omdat je vindt dat die persoon op de hoogte moet zijn van de inhoud, zorg dan dat je de gegevens van de zender verwijdert tenzij die persoon rechtstreeks moet communiceren met de afzender.
- 4.3 Informatie van internet kan virussen of malware bevatten. Beperk je internetgebruik tot het noodzakelijke en download alleen bestanden van betrouwbare herkomst.
- 4.4 Wees bedacht op verdachte 'phishing' e-mails. Klik niet op links in deze e-mails en geef geen logingegevens af. Op internet vind je meer informatie hoe je een verdachte mail herkent.

- 4.5 Deel geen vertrouwelijke informatie via onbeveiligde media zoals e-mail, sms, of filessharing applicaties zoals Dropbox of Google Drive.
- 4.6 Plaats geen vertrouwelijke gegevens van derden op sociale netwerken zoals Facebook, Twitter of LinkedIn.
- 4.7 Let erop als je deelneemt aan een sociaal netwerk dat de **NMFF's** niet geschaad worden door wat je plaatst.

5. Meld datalekken

Vanaf 1-1-2015 zijn de NMFF's verplicht om "ernstige datalekken" te melden bij het AP (Autoriteit persoonsgegevens). Dus bijvoorbeeld een verloren USB-stick met persoonsgegevens moet gemeld worden, ongeacht of er misbruik van de gegevens gemaakt is. Wees eerlijk en transparant en meld het via je secretariaat aan AP mochten er gegevens "op straat komen te liggen". Geef het lek ook door aan het secretariaat van de koepel zodat we landelijk een overzicht hebben en van zwakke punten kunnen leren.

6. Spreek collega's aan op onveilig gedrag

- 6.1 Bespreek zaken die je niet vertrouwt met een collega en bepaal samen welke actie je onderneemt.
- 6.2 Help collega's door ze te attenderen op situaties waarin onveilig gehandeld wordt op het gebied van het verwerken van persoonsgegevens.

7. Geef je mening over hoe gegevensbescherming veiliger kan

- 7.1 Draag verbeterpunten aan (via intranet) bij de projectgroep gegevensbeveiliging om verlies of misbruik van informatie te voorkomen.
- 7.2 Je ICT-omgeving verandert regelmatig. Denk actief mee over veiligheid van gegevens bij ingebruikname van bijvoorbeeld een nieuw systeem of een nieuwe online dienst.
- 7.3 Wees alert ('security aware').

8. Extra aandachtspunten (met name voor Secretariaat / Marketing / Communicatie)

- 8.1 Verzamel niet meer gegevens dan voor het doel noodzakelijk zijn.
- 8.2 Beschrijf (vooraf) in je privacy statement met welk doel je gegevens verzamelt.
- 8.3 Voor het verwerken van gegevens van jongeren onder de 16 jaar is schriftelijke toestemming van de ouder/voogd vereist.
- 8.4 Maak op je website duidelijk hoe iemand zijn persoonsgegevens kan inzien, corrigeren en verwijderen.
- 8.5 Corrigeer of verwijder de gegevens van een persoon als deze daarom vraagt. Uitzondering is als er wettelijke verplichtingen bestaan om dat niet te doen, bijv. i.v.m. wetgeving belasting.
- 8.6 Controleer periodiek de persoonsgegevens op juistheid.

- 8.7 Vernietig de persoonsgegevens als deze niet langer noodzakelijk zijn voor de doelstellingen van de gegevensverzameling.
- 8.8 Weeg steeds het belang van de **NMFF** af tegen de inbreuk op de privacy van de relatie.
- Je mag persoonsgegevens registreren als er sprake is van een gerechtvaardigd belang. Een normale bedrijfsvoering en marketingactiviteiten vallen hier ook onder. Vraag jezelf steeds af of je het doel ook kunt bereiken zonder verwerking van persoonsgegevens of met minder persoonsgegevens. Denk vanuit degene die je benadert: hoe zou je het zelf vinden als je op deze manier benaderd werd? Bestaat er een kans dat mensen de mailing/benadering ongepast vinden? Zo ja, vraag dan vooraf eerst toestemming.
- 8.9 Je mag gegevens altijd vastleggen als je toestemming hebt gekregen. Deze toestemming moet dan wel: vooraf gegeven zijn, vrijelijk afgegeven zijn (geen vooraangevinkte vakjes), afgegeven zijn met een actieve handeling (bijv. schriftelijk of door een vinkje te plaatsen; stilzwijgen of geen actie is geen toestemming), duidelijk omschreven zijn (concrete omschrijving van het doel en met wie de gegevens gedeeld worden).
- 8.10 Je mag persoonsgegevens delen met derden, zolang het verenigbaar is met het doel waarvoor de gegevens zijn verzameld. Vermeld in je privacyverklaring met wie je welke gegevens deelt en voor welk doel. Zorg dat er steeds sprake is van een gerechtvaardigd belang of toestemming.
- 8.11 Als iemand die niet bij de **NMFF** werkt gegevens van de **NMFF** verwerkt, is een bewerkersovereenkomst verplicht. Besef dat er al gauw sprake is van 'verwerken' van persoonsgegevens: het inzien van de gegevens door een externe helpdesk is al een verwerking.

Overtredingen en sancties

1. Rapporteer overtredingen aan je leidinggevende - Meld gedrag dat in strijd is met deze code, of sterke vermoedens van zulk gedrag, direct bij de directeur.
2. Gebruik de klokkenluiderregeling indien noodzakelijk - Maak gebruik van de klokkenluiderregeling (zie bijlage bij integriteitsbeleid) als de directeur niet adequaat reageert op een melding of als je melding juist het gedrag van de directeur betreft.

3. Overtredingen worden gesanctioneerd – Overtreed je de regels uit deze code, dan zijn verschillende sancties mogelijk, afhankelijk van de ernst van de overtreding. Sancties kunnen variëren van een waarschuwing tot ontslag op staande voet. Onverlet een eventuele eis tot schadevergoeding of aangifte bij de justitiële autoriteiten

Handtekening

Ik heb kennis genomen van de Gedragscode Natuur en Milieufederatie Flevoland en zal mij daaraan houden. Deze regelingen zijn mij bij de start van mijn werkzaamheden uitgereikt dan wel vooraf toegezonden.

(werknemer)

(plaats, datum)

Natuur en Milieufederatie Flevoland
Botter 11-47 (bezoekadres Botter 11-55
8232 JS Lelystad

info@nmfflevoland.nl
www.nmfflevoland.nl

0320-253505

NL35 INGB 0006 9313 98
KvK 40061700

