*Bijlage 3 bij het privacyreglement van De Nieuwe Veste*

# Gedragscode ICT De Nieuwe Veste

## Inleiding

*Deze gedragscode geeft aan wat passend gebruik van ICT middelen waaronder e-mail, internet en clouddiensten en sociale media is voor medewerkers en leerlingen van De Nieuwe Veste.*

Deze gedragscode bevat regels voor medewerkers en leerlingen met betrekking tot verantwoord gebruik van ICT middelen waaronder e-mail, internet en clouddiensten en het gebruik van de sociale media.

Onder ICT middelen wordt verstaan: alle middelen die een rol vervullen in informatie- en communicatieprocessen. Het gaat hierbij onder meer om computers, laptops, tablets, (mobiele) telefoons, printers, informatiedragers, kopieerapparatuur, scanners, fax-apparatuur, modems, internettoegang, e-mail en programma's/computersoftware.

Sociale media is uitgewerkt in een apart deel vanwege de specifieke aard.

De code bevat regels over de manier waarop controle op dit gebruik kan plaatsvinden, zonder daarmee de rechten van medewerkers en leerlingen te schaden of wettelijke bepalingen in het gedrang te brengen. De gedragscode heeft de intentie alle betrokkenen duidelijk te maken waar zij aan toe zijn en aan welke regels zij zich dienen te houden.

Deel 1: gebruik ICT middelen
De gedragscode bepaalt dat naast het zakelijke mailverkeer ook beperkt privé-verkeer is toegestaan, mits dit niet belemmerend is voor de dagelijkse werkzaamheden.

De code bestempelt specifieke handelingen als 'verboden', zoals het verzenden van berichten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud. Dit geldt ook voor het mailen van (seksueel) intimiderende berichten of boodschappen die aanzetten tot haat of geweld. Voor het internet geldt een verbod op het bezoeken van sites en het downloaden van materiaal met dergelijke aanstootgevende elementen.

Daarnaast bevat de code regels over de manier waarop controle op dit gebruik kan plaatsvinden, zonder daarmee persoonlijke rechten te schaden of wettelijke bepalingen in het gedrang te brengen. De gedragscode heeft de intentie alle betrokkenen duidelijk te maken waar zij aan toe zijn en aan welke regels zij zich dienen te houden.

De gebruikers van ICT middelen binnen De Nieuwe Veste mogen er vanuit gaan dat alle gegevens als eigendom van De Nieuwe Veste mogen worden beschouwd. Echter is inzage in de gegevens vanuit controle niet onbeperkt. Er worden voorwaarden gesteld aan controlerende acties. Zo is bepaald dat er in eerste instantie alleen controle plaatsvindt op basis van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen en dat de controle (tijdelijk) gerichter mag worden, zodra iemand ervan wordt verdacht de regels te overtreden.

Deel 2: gebruik sociale media
Het gebruik van sociale media is dusdanig specifiek dat dit apart geregeld is binnen de gedragscode. Sociale media spelen een belangrijke rol in het leven en het onderwijs. Sociale media betreft programma's waarmee online informatie kan worden opgezocht, gedeeld en gepresenteerd. Denk

bijvoorbeeld aan Facebook, Twitter, Instagram, YouTube, Snapchat maar ook alle (nieuwe) hiermee vergelijke programma's en apps.

Sociale media kunnen helpen om het onderwijs te verbeteren en de lessen leuker te maken, om contact te houden met vrienden en te experimenteren en grenzen te verleggen. Sociale media zoals Instagram, Facebook, YouTube en Twitter bieden de mogelijkheid om te laten zien dat je trots bent op je school en kunnen een bijdrage leveren aan een positief imago van De Nieuwe Veste. Van belang is te beseffen dat je met berichten op sociale media (onbewust) de goede naam van de school en betrokkenen ook kunt schaden. Om deze reden vragen wij om bewust met de sociale media om te gaan.

Essentieel is dat, net als in communicatie in de normale wereld, de gebruikers van sociale media de reguliere fatsoensnormen (niet pesten, kwetsen, stalken, bedreigen, zwartmaken of anderszins beschadigen) in acht blijven nemen en de nieuwe mogelijkheden met een positieve instelling benaderen.

De Nieuwe Veste vertrouwt erop dat zijn medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen verantwoord om zullen gaan met sociale media.

# Deel 1: gebruik ICT middelen De Nieuwe Veste

## 1. Uitgangspunten

1. Deze richtlijnen dragen bij aan een goed en veilig school- en onderwijsklimaat.
2. Deze richtlijnen bevorderen dat de instelling, medewerkers, leerlingen en ouders op een goede manier omgaan met ICT middelen waaronder e-mail en internet en bij het gebruik de reguliere fatsoensnormen (niet pesten, kwetsen, stalken, bedreigen, zwartmaken of anderszins beschadigen) hanteren. In de regel betekent dit dat we respect voor de school en elkaar hebben en iedereen in zijn waarde laten.
3. De controle op het gebruik van ICT middelen waaronder e-mail- en internet wordt conform deze gedragscode uitgevoerd. Indien er zich situaties voordoen waarin deze code niet voorziet, vindt overleg met de Medezeggenschapsraad plaats.
4. Er wordt gestreefd naar een goede balans tussen verantwoord gebruik van ICT middelen waaronder e-mail- en internet en bescherming van de privacy.
5. De Nieuwe Veste treft voorzieningen over de positie en integriteit van de medewerkers van de afdeling ICT en de controle daarop.

## 2. Doelgroep en reikwijdte

1. Deze richtlijnen zijn bedoeld voor alle betrokkenen die deel uitmaken van de schoolgemeenschap, dat wil zeggen medewerkers, leerlingen, ouders/verzorgers en mensen die op een andere manier verbonden zijn aan De Nieuwe Veste.
2. De richtlijnen hebben betrekking op verantwoord gebruik van ICT middelen waaronder e-mail- en internet en over de wijze waarop de controle daarop plaatsvindt.
3. De controle op persoonsgegevens over gebruik van ICT middelen waaronder e-mail en internet vindt plaats met als doel:
   - begeleiding / individuele beoordeling;
   - voorkomen van negatieve publiciteit;
   - tegengaan van seksuele intimidatie;
   - controle op bedrijfsgeheimen;
   - systeem en netwerkbeveiliging;
   - kosten en capaciteitsbeheersing;
   - tegengaan van discriminatie;
   - handelingen in strijd met het auteursrecht;
   - meldplicht datalekken.

## 3. E-mail- en internetgebruik

1. Het e-mail systeem en het internet worden voor school gebruik beschikbaar gesteld. Gebruik is derhalve verbonden aan functies en rollen.
2. Beperkt persoonlijk gebruik van het e-mailsysteem en het internet is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik in de zin van artikel 4 oplevert.

## 4. Verboden e-mail- en internetgebruik

1. Het is niet toegestaan om het e-mailsysteem te misbruiken of te gebruiken voor het verzenden van berichten met een pornografische, racistische, discriminerende, (seksueel) intimideren, beledigende of aanstootgevende inhoud of berichten die (kunnen) aanzetten tot haat en/of geweld. Het is niet toegestaan om op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten en/of dergelijk materiaal te downloaden.

2. Het is niet toegestaan om het e-mail systeem te gebruiken voor het verzenden van berichten die inbreuk maken op het auteursrecht. Het is niet toegestaan om op internet sites te bezoeken die inbreuk maken op het auteursrecht en/of dergelijk materiaal te downloaden.
3. Het is niet toegestaan om op internet sites te bezoeken voor online gokken en/of dergelijk materiaal te downloaden.
4. Het is niet toegestaan om zich ongeoorloofd toegang tot niet openbare bronnen op internet te verschaffen.

## 5. Gebruik netwerksysteem

1. Het netwerksysteem wordt voor school gebruik beschikbaar gesteld. Gebruik is derhalve verbonden aan functies en rollen.
2. Beperkt persoonlijk gebruik van het netwerk is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik in de zin van artikel 6 oplevert.
3. Belangrijke gegevens dienen (minimaal) opgeslagen te worden op de persoonlijke opslagruimte en/of in Office 365.
4. Voor clouddiensten zoals Office 365 gelden de regels en voorwaarden van de aanbieder.
5. Gasten mogen (al dan niet met eigen apparatuur) gebruik maken van het netwerksysteem en dienen zich dan ook aan deze gedragscode te houden.

## 6. Verboden netwerkgebruik

1. Het is niet toegestaan software te downloaden of te installeren op het computer- en/of netwerksysteem.
2. De homedrive is in grootte beperkt. Het is niet toegestaan om onnodig (grote) bestanden te bewaren.
3. Alle accounts die door de school beschikbaar gesteld zijn, zijn strikt persoonlijk. Het is niet toegestaan informatie over gebruikersnaam of wachtwoord van een account aan derden te verstrekken, tenzij dit noodzakelijk is voor een adequate uitoefening van de werkzaamheden. In het laatste geval dient altijd eerste overlegd te worden met de ICT afdeling. Zowel medewerkers als leerlingen zijn verplicht al hetgeen te doen wat redelijkerwijs verlangd mag worden om misbruik van verstrekte accounts te voorkomen.

## 7. Gebruik ICT apparatuur

1. ICT apparatuur wordt voor school gebruik beschikbaar gesteld. Gebruik is derhalve verbonden aan functies en rollen.
2. Beperkt persoonlijk gebruik van genoemde ICT apparatuur is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden.
3. Ga netjes en verantwoordelijk om met ICT apparatuur. Bij onzorgvuldig gedrag kunnen de kosten verhaald worden op de gebruiker.
4. Storingen of defecten aan apparatuur worden direct gemeld.
5. Onnodig printen (in kleur) wordt vermeden.

## 8. Voorwaarden voor controle

1. Controle van persoonsgegevens over het gebruik van ICT middelen waaronder e-mail- en internet vindt slechts plaats in het kader van de in artikel 2 lid 3 genoemde doelen.
2. Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
3. Indien iemand wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden. Controle beperkt zich in beginsel tot verkeersgegevens van het gebruik van ICT middelen waaronder e-mail- en internet. Slechts bij zwaarwegende redenen vindt diepgaande controle plaats.

4. Verboden gebruik van ICT middelen waaronder e-mail- en internet wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Overige controle vindt slechts steekproefsgewijs plaats.
5. Bij constatering van verboden gebruik wordt dit onmiddellijk met de betrokkene besproken. De betrokkene wordt gewezen op de consequenties wanneer hij of zij niet stopt met het verboden gebruik.
6. E-mailberichten van leden van de MR onderling, van vertrouwenspersonen, bedrijfsartsen en van een ieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden niet in principe gecontroleerd. Dit geldt niet voor veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.
7. Het hoofd ICT kan ter voorkoming van onjuist gedrag en/of ter verhoging van het beveiligingsniveau onder andere de volgende maatregelen nemen:
   - ongewenste websites blokkeren (web-filtering);
   - ongewenste bestanden automatisch laten blokkeren (o.a. virussen);
   - ongewenste mail automatisch laten blokkeren (content-filtering);
   - downloaden beperken tot een bepaalde omvang gedurende een bepaalde periode.

## 9. Controle

1. De controle in het kader van begeleiding en/of individuele beoordeling vindt steekproefsgewijs plaats.
2. 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.
3. De controle op het uitlekken van bedrijfsgeheimen vindt plaats op basis van steekproefsgewijze content-filtering.
4. De uitvoering van controle vindt plaats door de afdeling ICT onder verantwoordelijkheid van het hoofd ICT. Het hoofd ICT wijst één of meerdere systeembeheerders aan die belast zijn met het beheer van het (de) bestand(en). Deze systeembeheerders zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennisnemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.
5. Door de verantwoordelijke worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
6. Door de verantwoordelijke worden passende technische en organisatorische maatregelen ten uitvoer gelegd om (persoons)gegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

## 10. Gerichte controle/onderzoek

1. Op basis van gerechtvaardigde vermoedens van onjuist gebruik, of na het constateren van onjuist gebruik, kan een gericht onderzoek worden ingesteld door de ICT afdeling onder verantwoordelijkheid van het hoofd ICT. De schriftelijke opdracht tot het verrichten van een gericht onderzoek kan uitsluitend worden gegeven door de afdelingsdirecteur of direct leidinggevende. Het onderzoek blijft beperkt tot het verzamelen van gegevens over het gebruik van ICT-middelen. In dit stadium kan geen onderzoek naar de inhoud van e-mailberichten of bestanden plaatsvinden. Het hoofd ICT geeft in een schriftelijk verslag aan de opdrachtgever het resultaat van het onderzoek weer. De betrokkene en het CMT ontvangen een afschrift van het verslag. Als het onderzoek geen aanleiding geeft tot verdere maatregelen, wordt het verslag vernietigd, evenals alle verzamelde gegevens.
2. Bij zwaarwegende redenen kan de afdelingsdirecteur of direct leidinggevende besluiten bij een nader gericht onderzoek ook de inhoud van e-mails of bestanden te betrekken. De directeur vermeldt in de schriftelijke opdracht aan het hoofd ICT de redenen voor het onderzoek.
3. De betrokkene naar wie een gericht onderzoek wordt ingesteld, wordt hiervan door de opdrachtgever van het onderzoek op de hoogte gesteld de start van het onderzoek. Als de omstandigheden daartoe aanleiding geven, kan eerst een nader gericht onderzoek naar onjuist gebruik van ICT-middelen worden ingesteld, voordat de betrokkene op de hoogte wordt gebracht.

Binnen vier weken na ontvangst van het verslag wordt de betrokkene door de opdrachtgever in de gelegenheid gesteld uitleg te geven over geconstateerd onjuist gebruik.

4. Binnen vier weken na het gesprek met de betrokkene beslist de directeur over het eventueel opleggen van een sanctie. De beslissing wordt schriftelijk meegedeeld.

## 11. Sancties en gevolgen voor medewerkers en leerlingen

1. Medewerkers die in strijd handelen met deze richtlijnen maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het personeelsdossier.
2. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar medewerkers toe rechtspositionele maatregelen genomen welke variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet.
3. Leerlingen en / of ouders/verzorgers die in strijd met deze richtlijnen handelen maken zich mogelijk schuldig aan verwijtbaar gedrag. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het leerlingendossier.
4. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar leerlingen en / of ouders/verzorgers toe maatregelen genomen welke variëren van waarschuwing, schorsing en verwijdering van school
5. Indien de uitlating van leerlingen, en/of ouders/verzorgers en medewerkers mogelijk een strafrechtelijke overtreding inhoudt zal door de directie aangifte bij de politie worden gedaan.

## 12. Persoonsgegevens

1. Elektronisch vastleggen van persoonsgegevens geschiedt (automatisch) door de ingezette software.
2. De vastlegging beperkt zich tot de noodzakelijke gegevens.
3. De persoonsgegevens worden maximaal zes maanden bewaard. Gegevens die ouder zijn dan zes maanden worden automatisch verwijderd, tenzij er een redelijk vermoeden bestaat van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen in die periode. In dat geval worden de gegevens uit die betreffende zes maanden bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een betrokkene noodzakelijk is. Zodra een nader onderzoek is afgerond en dit niet leidt tot maatregelen jegens een betrokkene worden de gegevens verwijderd.
4. Indien de afdeling ICT om technische redenen persoonsgegevens niet kan verwijderen, wordt onder verwijderen verstaan het niet meer verstrekken van deze gegevens voor de in artikel 2 geformuleerde doeleinden.
5. Voor de regeling ‘meldingsplicht datalekken’ van de Algemene Verordening Gegevensbescherming (AVG) is een procedure opgesteld. Iedereen wordt geacht (ernstige) ongeregeldheden waar persoonsgegevens mee gemoeid zijn te melden bij de ICT afdeling.

# Deel 2: gebruik sociale media De Nieuwe Veste

## 1. Uitgangspunten

1. De Nieuwe Veste onderkent het belang van sociale media.
2. Deze richtlijnen dragen bij aan een goed en veilig school- en onderwijsklimaat.
3. Deze richtlijnen bevorderen dat de instelling, medewerkers, leerlingen en ouders op de sociale media communiceren in het verlengde van de missie en visie van de onderwijsinstelling en de reguliere fatsoensnormen. In de regel betekent dit dat we respect voor de school en elkaar hebben en iedereen in zijn waarde laten.
4. De gebruikers van sociale media dienen rekening te houden met de goede naam van de school en van een ieder die betrokken is bij de school.
5. Deze richtlijnen dienen de onderwijsinstelling, haar medewerkers, leerlingen en ouders tegen zichzelf en anderen te beschermen tegen de mogelijke negatieve gevolgen van de sociale media.

## 2. Doelgroep en reikwijdte

1. Deze richtlijnen zijn bedoeld voor alle betrokkenen die deel uitmaken van de schoolgemeenschap, dat wil zeggen medewerkers, leerlingen, ouders/verzorgers en mensen die op een andere manier verbonden zijn aan De Nieuwe Veste.
2. De richtlijnen hebben enkel betrekking op school-gerelateerde berichten of wanneer er een overlap is tussen school, werk en privé.

## 3. Voor alle gebruikers (medewerkers, leerlingen en ouders/verzorgers)

1. Het is medewerkers en leerlingen niet toegestaan om tijdens de lessen actief te zijn op sociale media tenzij door de schoolleiding respectievelijk docenten hiervoor toestemming is gegeven.
2. Het is betrokkenen toegestaan om kennis en informatie te delen, mits het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen niet schaadt.
3. De betrokkene is persoonlijk verantwoordelijk voor de inhoud welke hij publiceert op de sociale media en kan daarop worden aangesproken. Ook het doorsturen (forwarden) en herplaatsen (retweeten) zijn handelingen waarop je aangesproken kunt worden.
4. Elke betrokkene dient zich ervan bewust te zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na verwijdering van het bericht. Het is daarom belangrijk om te zorgen dat instellingen goed staan en je niet meer informatie deelt dan je wilt.
5. Het is voor betrokkenen niet toegestaan om foto-, film- en geluidsopnamen van school-gerelateerde situaties op de sociale media te zetten tenzij betrokkenen hier uitdrukkelijk toestemming voor plaatsing hebben gegeven.
6. Het is medewerkers niet toegestaan om ‘vrienden’ te worden met leerlingen op sociale media tenzij het gaat om een door de medewerker gebruikt professioneel account (waar geen persoonlijke informatie over de medewerker is geplaatst).
7. De medewerkers mogen een WhatsApp groep maken met een groep leerlingen. Het is niet toegestaan om één of één contact met leerlingen te hebben via Whatsapp. Het WhatsApp contact in de groep moet altijd professioneel blijven en gaan over school-gerelateerde onderwerpen. Het contact in de WhatsApp groep moet voor alle deelnemers aan de groep openbaar zijn. Ter bescherming van zowel de docent als de leerlingen worden gesprekken in de WhatsApp groep niet gewist en kan de leidinggevende de gespreksgeschiedenis van de WhatsApp groep opvragen.
8. Alle betrokkenen nemen de fatsoensnormen in acht. Als fatsoensnormen worden overschreden (bijvoorbeeld: mensen pesten, kwetsen, stalken, bedreigen, zwartmaken of anderszins beschadigen) dan nemen wij passende maatregelen. Zie ook : *Sancties en gevolgen voor medewerkers en leerlingen*

9. Als er gebruik wordt gemaakt van het netwerk van de school, dan mag dat de kwaliteit van het (draadloze) netwerk niet in gevaar brengen of schade aan personen of instellingen veroorzaken. Het hacken, overmatig downloaden of overbelasten van het netwerk is natuurlijk verboden.
10. Internet en sociale media worden alleen gebruikt voor acceptabele doeleinden. Het is daarom niet toegestaan om op school:
    a. sites te bezoeken informatie te downloaden en te verspreiden die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend zijn;
    b. hacken en ongeoorloofd toegang te krijgen tot niet-openbare sites of programma's;
    c. informatie, foto's of video's te delen waarvan duidelijk is dat die niet bedoeld is om verder te verspreiden, hou je wachtwoorden geheim;
    d. verzonnen berichten versturen of een fictieve naam gebruiken als afzender;
    e. iemand lastig vallen, te achtervolgen of te 'flamen'.

    Als iemand over de voorgaande punten informatie krijgt aangeboden, wordt dat gemeld aan de afdelingsdirecteur of de direct leidinggevende.

## 4. Voor medewerkers tijdens werksituaties

1. Medewerkers hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media: privémeningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van De Nieuwe Veste. Dit geldt extra voor medewerkers met een representatieve functie zoals leidinggevenden.
2. Indien een medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met De Nieuwe Veste, dient de medewerker te vermelden dat hij medewerker is van De Nieuwe Veste is.
3. Als online communicatie dreigt te ontsporen dient de medewerker direct contact op te nemen met zijn leidinggevende om de te volgen strategie te bespreken.
4. Bij twijfel of een publicatie in strijd is met deze richtlijnen neemt de medewerker contact op met zijn leidinggevende.

## 5. Voor medewerkers buiten werksituaties

1. Het is de medewerker toegestaan om school-gerelateerde onderwerpen te publiceren mits het geen vertrouwelijke of persoonsgebonden informatie over de school, zijn medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen betreft. Tevens mag de publicatie de naam van de school niet schaden.
2. Indien de medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met de onderwijsinstelling dient medewerker te vermelden dat hij medewerker is van De Nieuwe Veste.
3. Indien de medewerker over De Nieuwe Veste publiceert dient hij het bericht te voorzien van het bericht dat de standpunten en meningen in dit bericht de eigen persoonlijke mening zijn en los staan van eventuele officiële standpunten van De Nieuwe Veste. Verder meldt de medewerker dat hij of zij niet verantwoordelijk is voor de inhoud en uitlatingen van derden.

## 6. Sancties en gevolgen voor medewerkers en leerlingen

1. Medewerkers die in strijd handelen met deze richtlijnen maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het personeelsdossier.
2. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar medewerkers toe rechtspositionele maatregelen genomen welke variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet.
3. Leerlingen en / of ouders/verzorgers die in strijd met deze richtlijnen handelen maken zich mogelijk schuldig aan verwijtbaar gedrag. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het leerlingendossier.

4. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar leerlingen en / of ouders/verzorgers toe maatregelen genomen welke variëren van waarschuwing, schorsing en verwijdering van school
5. Indien de uitlating van leerlingen, en/of ouders/verzorgers en medewerkers mogelijk een strafrechtelijke overtreding inhoudt zal door de directie aangifte bij de politie worden gedaan.