

Reglement voor het gebruik van elektronische communicatiemiddelen door leerlingen

De Stichting Openbaar Voortgezet Onderwijs Ooststellingwerf, gevestigd te Oosterwolde.

Gelet op,

De Wet Bescherming Persoonsgegevens en
Artikel 6 lid c en artikel 8.1, lid d van de Wet Medezeggenschap Onderwijs

Overwegende dat,

het gebruik van elektronische communicatiemiddelen waaronder internet en e-mail voor de leerlingen binnen Het Stellingwerf College nodig wordt geacht voor het onderwijsproces,

aan het gebruik van internet risico's verbonden zijn die nopen tot het stellen van gedragsregels,

tegen de achtergrond van deze risico's van de leerlingen verantwoord gebruik van elektronische communicatiemiddelen wordt verwacht,

het Stellingwerf College gerechtigd is tot het geven van voorschriften voor gebruik van elektronische communicatiemiddelen en het nemen van maatregelen ter bevordering van de goede orde in de onderneming (artikel 7:660 BW),

de onderhavige gedragscode voorschriften en maatregelen bevat zoals hiervoor genoemd,

het Stellingwerf College gerechtigd is persoonsgegevens te verwerken ten behoeve van de controle op de naleving van deze gedragscode,

het Stellingwerf College bij de controle de fundamentele rechten en vrijheden van de betrokken werknemer(s) in acht neemt, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer (artikel 8 sub f WBP),

heeft met instemming van de medezeggenschapsraad de volgende gedragscode vastgesteld.

Artikel 1. Begripsbepaling

1. School: Stichting Openbaar Voortgezet Onderwijs Ooststellingwerf , waartoe behorend het Stellingwerf College.
2. MR: Medezeggenschapsraad
3. WBP: Wet Bescherming Persoonsgegevens
4. Directie: Directie van de school .
Leerlingen: Leerlingen van bovengenoemde school.
Leerlingen die tijdelijk op school aanwezig zijn b.v. in het kader van uitwisseling.
5. Elektronische communicatiemiddelen: door of namens de school aan leerlingen ter beschikking gestelde computer-, e-mail, en/of netwerkfaciliteiten, telefoons, gsm, pda etc.
6. Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van de WBP.
7. Onrechtmatig gebruik / misbruik van elektronische communicatiemiddelen: een doen of nalaten in strijd met dit reglement of een andere wet- en regelgeving of een inbreuk op een recht.
8. Netwerkfaciliteiten: door of namens de school aan leerlingen ter beschikking gestelde netwerkfaciliteiten; waaronder schoolnetwerk, dan wel internet, intranet of extranet.

Artikel 2. Doel van de afspraken

1. Deze regeling geeft de wijze aan waarop in de organisatie wordt omgegaan met elektronische communicatiemiddelen. Deze omvat gedragsregels ten aanzien van verantwoord gebruik van elektronische communicatiemiddelen en regels over de wijze waarop controle op misbruik plaats vindt.
2. De controle op persoonsgegevens over e-mail en netwerkgebruik vindt plaats met als doel in elk geval:
 - a. het verzamelen van bewijs,
 - b. het opbouwen van archiefmateriaal
 - c. het voorkomen van discriminatie en seksuele intimidatie
 - d. het naleven van afspraken over verboden gebruik
 - e. het beheersen van kosten en capaciteit
 - f. het beveiligen van systeem en netwerk
 - g. het voorkomen van negatieve publiciteit
 - h. het meewerken aan onderzoeken door justitie

Artikel 3. Algemene uitgangspunten

1. Gestreefd wordt naar een goede balans tussen controle op verantwoord gebruik van elektronische communicatiemiddelen en bescherming van de privacy van leerlingen op de werkplek.
2. Persoonsgegevens over e-mail en netwerkgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn zoals door de wet voorgeschreven.
3. De werkgever maakt bindende werkafspraken met de systeembeheerder(s) en applicatiebeheerder(s) over zaken als geheimhouding en privacybescherming m.b.t. de school en allen die daarin werken.

Artikel 4. Gebruik elektronische communicatiemiddelen

1. De elektronische communicatiemiddelen zijn door de school aan de leerlingen ter beschikking gesteld voor de uitvoering van hun schooltaken, en mogen in beginsel uitsluitend voor die doeleinden gebruikt worden.
2. Leerlingen mogen zich slechts onder de eigen inlognaam toegang verschaffen tot het netwerk, de mail en de internetvoorzieningen.
3. Beperkt privé-gebruik van de elektronische communicatiemiddelen is toegestaan, mits het wordt beperkt tot kortdurend gebruik en het niet storend is voor andere gebruikers, het netwerk dan wel de uit te voeren taken.
4. Het is verboden de elektronische communicatiemiddelen te gebruiken/misbruiken voor doeleinden waarvoor zij niet bestemd zijn. In ieder geval is het volgende aan leerlingen verboden:
 - a. het doen van handelingen die bij wet verboden zijn;
 - b. het bekijken of verspreiden van pornografisch en/of gewelddadig materiaal;
 - c. het doen van discriminerende of seksueel intimiderende uitingen;
 - d. verrichtingen die volgens de gebruikersovereenkomst niet zijn toegestaan.
5. Voor het gebruik van e-mail, internetfaciliteiten of andere elektronische communicatiemiddelen geldt dat leerlingen worden geacht respectvol naar elkaar en naar het personeel te zijn.

Artikel 5. Controle

1. Controle op gebruik van elektronische communicatiemiddelen en controle op de automatisch geregistreerde gegevens vindt slechts plaats in het kader van in artikel 2.2 genoemde doelen.
2. Registratie van gegevens vindt in beginsel plaats op het niveau van getotaliseerde geregistreerde gegevens die niet herleidbaar zijn tot een individuele leerling. Indien een leerling of een groep leerlingen van onrechtmatig gebruik/misbruik van elektronische communicatiemiddelen wordt verdacht, kan gedurende een vastgestelde (korte) periode persoonlijk gerichte controle plaats vinden. De directie neemt hiertoe het besluit.
3. De inhoud van e-mailberichten van leden van de MR en zorgfunctionarissen wordt niet gecontroleerd.

4. Controle beperkt zich in principe tot verkeersgegevens van het gebruik van elektronische communicatiemiddelen. Alleen bij zwaarwegende redenen (zie artikel 5.2) vindt er controle op de inhoud plaats. Betreft deze controle een vertrouwenspersoon zoals bedoeld in artikel 5.3, dan vindt deze plaats door een vertrouwenspersoon van een andere school.
5. De school neemt maatregelen in technische zin om onrechtmatig gebruik of misbruik van elektronische communicatiemiddelen te voorkomen.
6. Programma's en bestanden die niet op de systemen van de school thuishoren kunnen worden verwijderd in opdracht van de directie.
7. Leerlingen ten aanzien van wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door een lid van de directie of een daartoe aangestelde medewerker op hun gedrag aangesproken.
8. Bij het werken op leerlingen PC's is het mogelijk dat naleving van de geldende regels steekproefsgewijs via schermmonitoring wordt gecontroleerd.

Artikel 6. Rechten van de betrokkenen

1. De school informeert de leerlingen voorafgaand aan de invoering van het reglement voor het gebruik van elektronische communicatiemiddelen, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.
2. Bij de in artikel 5.2 en 5.3 genoemde persoonlijke controle worden ten hoogste de volgende persoonsgegevens opgenomen:
 - a. gebruikersidentificatie, naam, voornaam of voorletters van de betrokkene;
 - b. naam en/of codering van de locatie, school waaronder betrokkene valt;
 - c. gegevens over de toegang tot internet en netwerkfaciliteiten die door de school zijn geboden aan de leerling, inclusief gebruikersnaam en internet protocoladres;
 - d. gegevens betreffende de datum en het tijdstip van het openen en sluiten van de toegang tot internet door de betrokkene en gegevens betreffende de datum en het tijdstip van het verzenden, dan wel ontvangen van e-mailberichten door de betrokkene;
 - e. gegevens, inclusief datum en tijdstip, betreffende de door de betrokkene bezochte internetsites (internet protocoladressen en (de onderdelen van) de webpagina's;
 - f. de inhoud van de door de betrokkene verzonden, dan wel ontvangen e-mailberichten.
3. Leerlingen kunnen zich tot de school wenden met het verzoek om een volledig overzicht van hun verwerkte persoonsgegevens. Het verzoek wordt binnen 4 weken beantwoord.
4. Leerlingen kunnen de school verzoeken hun persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend, dan wel in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek wordt binnen 4 weken beantwoord.
5. Leerlingen kunnen bij de directie verzet aantekenen tegen de verwerking van hun persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. De directie oordeelt binnen 4 weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien de directie het verzet gerechtvaardigd acht, beëindigt hij terstond de verwerking.

Artikel 7. Sancties

Leerlingen kunnen bij overtreding van dit reglement worden bestraft conform het school- dan wel het leerlingenreglement .

Artikel 8. Onvoorziene omstandigheden

In gevallen waarin dit reglement niet voorziet of bij twijfel omtrent de toepassing van dit reglement beslist de algemene directie.

Artikel 9. Slotbepaling

1. De directie kan deze regeling met instemming van de MR wijzigen. Deze wijzigingen worden schriftelijk vastgelegd en voorafgaand aan de invoering aan de leerlingen bekend gemaakt.
2. Deze regeling is tot stand gekomen in overleg en met instemming van de MR bij besluit van d.d. 28 juni 2005

Toelichting

Algemeen

De invoering van een Reglement voor het gebruik van elektronische communicatiemiddelen is een besluit waarvoor de instemming van de MR nodig is (Artikel 6 lid c en artikel 8, lid d van de Wet Medezeggenschap Onderwijs).

In dit reglement staan voorbeelden van verboden e-mail- en netwerkgebruik en van verantwoord gebruik van het e-mail- en netwerksysteem. Hierbij is het uiteraard van belang, dat vooraf bekend is wat wel en wat niet is toegestaan. Wanneer de directie een controlemaatregel wil invoeren dient hij eerst het doel voor de controlemaatregel bekend te maken.

Dit reglement is van toepassing op (geheel of gedeeltelijke) geautomatiseerde verwerking van persoonsgegevens van leerlingen van de school met betrekking tot de e-mail-, internet- en netwerkadministratie.

Artikel 1

Begripsbepaling

Artikel 2

Persoonsgegevens mogen slechts voor bepaalde en gerechtvaardigde doeleinden worden verzameld en niet worden verwerkt voor doeleinden die daarmee onverenigbaar zijn. De directie (verantwoordelijke) moet de doelen bepalen vóórdat hij begint met het verwerken van persoonsgegevens. Hierbij is van belang dat het doel van de verwerking zo nauwkeurig en volledig mogelijk wordt omschreven. Als er meerdere doelstellingen zijn, moeten deze afzonderlijk worden genoemd en getoetst op de noodzaak om persoonsgegevens te verzamelen. In overleg met de MR moet worden vastgesteld welke doeleinden voor controle van e-mail en internetgebruik noodzakelijk zijn voor de eigen organisatie. De privacybelangen van de leerlingen horen hierbij meegewogen te worden.

De doeleinden die in artikel 2.2 worden genoemd zijn niet limitatief. Echter, zodra de directie besluit tot uitbreiding van deze lijst, is hiervoor de instemming van de MR vereist. Hieronder volgt enige toelichting:

Voorkomen van discriminatie en seksuele intimidatie

Via elektronische communicatie kan eenvoudig seksuele intimidatie worden gepleegd. Een directie die het beleid hiervoor wil handhaven, kan deze communicatie onderwerpen aan een geautomatiseerde controle. Bijvoorbeeld kan een tekst gescand worden op verboden woorden en kunnen verdachte berichten (geautomatiseerd) worden teruggestuurd aan de oorspronkelijke afzender. Op die wijze kan de privacy van de leerlingen ongeschonden blijven.

Het naleven van afspraken over verboden gebruik

Zowel in dit reglement als in de toelichting wordt verboden gebruik omschreven. Doel van de controles is om dit gebruik op te sporen en te voorkomen.

Het beheersen van kosten en capaciteit

Uiteraard kost het versturen van data, in welke vorm dan ook, geld en legt het beslag op de beschikbare capaciteit van het netwerk. Deze vorm van controle kan beperkt blijven tot het controleren van de verkeersgegevens. Kennisneming van de inhoud van de mail is voor dit doel niet noodzakelijk.

Het beveiligen van systeem en netwerk

Vanuit beveiligingsoogpunt is het wenselijk om e-mail en ander dataverkeer te controleren. Het kan dan gaan om het tegengaan van systeemaanvallen door virussen of andere schadelijke programma's. Bij deze controle verdient een geheel geautomatiseerde controle van inkomende berichten en bijlagen de voorkeur. Indien een besmet bericht gevonden wordt, kan dit op een aparte locatie worden bewaard voor nader onderzoek en eventuele herstelwerkzaamheden.

Voorkomen van negatieve publiciteit

Leerlingen kunnen via elektronische communicatie de goede naam van de school behoorlijk aantasten. Het plegen van strafbare feiten, seksuele intimidatie of discriminerende uitingen kan immers geschieden onder gebruikmaking van het (e-mail/web)adres van de school. Het verdient de voorkeur hier de controle geheel geautomatiseerd te laten plaatsvinden middels content-filtering. Verdachte berichten – zowel inkomende als uitgaande – dienen zoveel mogelijk (geautomatiseerd) te worden teruggestuurd naar de afzender, waardoor vastlegging van de inhoud van het bericht niet nodig is.

Bij gebruik van het internetverkeer via vaste IP-adressen kan een bezoek aan een bepaalde internet-site altijd herleid worden tot een bepaalde organisatie. Om negatieve publiciteit te voorkomen, kan de directie het internetgebruik steekproefsgewijs controleren.

Meewerken aan onderzoeken door justitie

Wanneer er bij justitie aangifte wordt gedaan van discriminatie of seksuele intimidatie en justitie redenen heeft aan te nemen dat deze verzonden zijn vanaf elektronische communicatieapparatuur op de school, kan justitie de school verzoeken mee te werken aan een onderzoek. De school zal hieraan gevolg moeten geven en de gevraagde gegevens moeten verstrekken.

Artikel 3

De hoofdregel van de Wet Bescherming Persoonsgegevens eist dat persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de wet worden verwerkt.

De WBP kent een ruime betekenis toe aan het begrip 'verwerking van persoonsgegevens'. Hieronder wordt verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Een persoonsgegeven in de zin van de WBP is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Het kan om allerlei soorten informatie gaan: om eigenschappen van de betrokkene, diens opvattingen of gedragingen. Meer in het algemeen gaat het om gegevens die bepalend kunnen zijn voor de manier waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.

Omdat de werknemers en eventuele stagiaires van de afdeling systeembeheer en applicatiebeheer uit hoofde van hun functie toegang hebben en moeten hebben tot een aantal basisgegevens en de systemen kunnen controleren, moet de integriteit van deze personen gewaarborgd zijn.

Artikel 4

In dit reglement worden gedragsregels opgenomen over wat niet toegestaan is bij een verantwoord gebruik van elektronische communicatie middelen. Andere voorbeelden van verboden gebruik zijn:

- Het downloaden of versturen van illegale software;
- Het inbreken op het eigen of op andere netwerken.
- Het zich toegang verschaffen op het netwerk met de accountnaam van een ander.
- Het downloaden of versturen van omvangrijke bestanden die veel beslag leggen op de beschikbare capaciteit, zoals video en audiobestanden, zonder overleg met de systeembeheerder;
- Het online gokken
- Het versturen van sms- of e-mailberichten met een dreigende inhoud.
- Misbruik van mobiele telefoon en/of pda, waaronder die met camera.

Leerlingen mogen de elektronische communicatiemiddelen kortstondig voor persoonlijke doeleinden gebruiken, mits dit niet storend is voor andere gebruikers, het netwerk dan wel de uit te voeren taken. Een totaal verbod op het internetgebruik voor persoonlijke doeleinden is niet mogelijk en niet wenselijk.

Artikel 5

Veel gegevens worden door de systemen automatisch geregistreerd zonder dat er een controle plaatsvindt. Dit kunnen zijn: laatste inlogtijdstip, IP-nummer, bezochte sites et cetera.

Afhankelijk van het doel worden de omvang en wijze van controle aangepast.

E-mailberichten van leden van de ondernemingsraad mogen niet worden gecontroleerd. Dit geldt eveneens voor andere in de onderneming werkzame personen, waaronder zorgfunctionarissen.

De school neemt een aantal maatregelen ter voorkoming van misbruik. Deze kunnen bijvoorbeeld bestaan uit: content-filtering (het scannen van berichten of bestanden op verboden woorden of extensies); het afsluiten van bepaalde (verboden of ongewenste) websites; het afsluiten van bepaalde (verboden of ongewenste) nieuwsgroepen; het stoppen van doorgiften of gebruikersanalyses. Programma's en bestanden die in het kader hiervan niet op de systemen thuis horen, kunnen worden verwijderd.

Schermonitoring kan plaatsvinden met speciaal voor dit doel ontworpen schoolsoftware. Dit kan gebeuren door een docent in een klassensituatie maar ook door de afdeling systeembeheer

Artikel 6

De betrokken leerling heeft het recht zich vrijelijk en met redelijke tussenpozen tot zijn directie te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De directie deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt. De betrokken leerling kan de directie verzoeken de hem/haar betreffende persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze gegevens:

- onjuist zijn
- voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn
- dan wel anderszins in strijd met een wettelijk voorschrift of met deze gedragscode zijn verwerkt

De directie bericht de verzoeker (leerling) binnen vier weken na ontvangst van het verzoek schriftelijk in hoeverre hij aan het verzoek zal voldoen. Een weigering is met redenen omkleed. De directie draagt er zorg voor, dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

Artikel 7

Alle leerlingen waarvoor dit reglement van toepassing is worden gehouden aan de plichten zoals omschreven in dit reglement. Geconstateerde overtredingen kunnen leiden tot het nemen van sancties.