



## **GEDRAGSCODE ICT: INTERNET EN EMAILGEBRUIK**

STELLER : Rien van Heukelom  
 TELNR. : 077-3590511  
 EMAIL. : rvheukelom@ogvo.nl  
 DATUM : 16 april 2012

### **Gedragcode internetgebruik van de Onderwijsgemeenschap Venlo & Omstreken**

#### **Deze Gedragcode geeft aan wat passend gebruik van internet en social media is voor medewerkers en leerlingen van Onderwijsgemeenschap Venlo & Omstreken**

Deze gedragscode bevat regels met betrekking tot verantwoord internet- en e-mailgebruik en gebruik van de social media. Het laatstgenoemde kent een aparte paragraaf vanwege de specifieke aard van deze media. Daarnaast bevat de code regels over de manier waarop controle op dit gebruik kan plaatsvinden, zonder daarmee de rechten van werknemers te schaden of wettelijke bepalingen in het gedrang te brengen. De gedragscode heeft de intentie alle betrokkenen (zowel werkgever als werknemer) duidelijk te maken waar zij aan toe zijn en aan welke regels zij zich dienen te houden.

Controle op handelingen van werknemers op het internet of op e-mailberichten die worden verzonden, is geen vanzelfsprekendheid en vergt primair instemming van de Gemeenschappelijke Medezeggenschapsraad (GMR) en vervolgens toestemming van Bevoegd Gezag. Deze zal enkel instemming verlenen indien het verzoek gepaard gaat met een duidelijk omschreven doel.

#### **Handleiding**

De gedragscode bepaalt dat naast het zakelijke mailverkeer ook beperkt privé-verkeer is toegestaan, mits dit niet belemmerend is voor de dagelijkse werkzaamheden. Ook kan de code specifieke handelingen als 'verboden' bestempelen, 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 kan ook een verbod gelden op het bezoeken van sites en het downloaden van materiaal met dergelijke aanstootgevende elementen. Het ligt voor de hand voorwaarden te stellen aan de controle: zo kan worden 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) gericht mag worden, zodra een werknemer (of werknemers) ervan wordt verdacht de regels te overtreden.

Ook moet de gedragscode heel duidelijk de doelen van een eventuele controle benoemen, zoals het 'voorkomen van negatieve publiciteit', 'controle op bedrijfsgeheimen' of bijvoorbeeld 'begeleiding of individuele beoordeling'. Datzelfde geldt voor de rechten van de werknemers; ook die moeten worden vastgelegd.

#### **Social Media**

Het gebruik van Social Media is dusdanig specifiek dat dit apart geregeld is binnen de gedragscode. Onderwijsgemeenschap Venlo & Omstreken ziet het gebruik van sociale media als een belangrijke maatschappelijke ontwikkeling. Net zoals bij de opkomst van internet ontstaan er nieuwe mogelijkheden en is niet altijd duidelijk hoe zaken geregeld moeten worden. Wij vertrouwen er echter op dat elke medewerker goed in staat is verstandige keuzes te maken. Met deze richtlijnen willen we alle medewerkers helpen sociale media optimaal te benutten en vervelende ervaringen voor de persoon en / of de organisatie voorkomen.

Als sociale media beschouwen we online platformen (communicatiekanalen) die het mogelijk maken dat mensen online hun mening kunnen ventileren, ervaringen kunnen delen en met elkaar in contact kunnen treden. Dit kan door zelf te publiceren of gebruik te maken van de aanwezige reactiemogelijkheden. De op dit moment bekendste sociale media in Nederland zijn Hyves,

Facebook, Twitter, LinkedIn, Foursquare en Youtube. Ook veel nieuwsmedia zijn tegenwoordig online actief waardoor je snel een reactie kunt plaatsen.

Elke campus beschikt over officiële accounts voor sociale media sites. Informatie *namens* Onderwijsgemeenschap Venlo & Omstreken en / of de campussen ('officiële' mededelingen) komen uitsluitend via deze kanalen tot gebruikers.

De geformuleerde richtlijnen hebben betrekking op persoonlijke activiteiten op sociale media, of deze nu op het werk of in je vrije tijd plaatsvinden en hebben de intentie om organisatie, medewerkers, leerlingen en ouders te beschermen tegen mogelijk negatieve gevolgen van het gebruik van sociale media. De formele regels die wij hanteren, hebben in beginsel betrekking op wat je onder werktijd en voor je werk doet. We kunnen en willen geen richtlijnen uitvaardigen die betrekking hebben op wat je privé doet. Wel vragen we iedereen, óók bij wat je als privépersoon doet, je ervan bewust te zijn dat het steeds makkelijker is voor anderen om te zien wie je bent en waar je werkt. Daarmee word je, in wat je in je eigen tijd als privépersoon doet, ook steeds meer beschouwd als een vertegenwoordiger van je eigen campus en Onderwijsgemeenschap Venlo & Omstreken . Wij gaan ervan uit dat je je daarvan bewust bent en je daar op een verantwoordelijke manier mee omgaat, zodat uitingen via sociale media in het verlengde van missie en visie van de Onderwijsgemeenschap passen en in lijn zijn met de reguliere fatsoensnormen.

Het is goed je te realiseren dat niet opeens alles nieuw en anders is. Zo blijft het van belang om altijd je gezond verstand te gebruiken. Realiseer je bijvoorbeeld dat informatie die je op sociale media sites zet niet meer verwijderd kan worden. Informatie die je alleen beschikbaar maakt voor "vrienden" kan makkelijk gekopieerd worden en beschikbaar komen voor de rest van de wereld.

**REGLEMENT EMAIL- EN INTERNETGEBRUIK**

De Onderwijsgemeenschap Venlo & Omstreken (OGV&O)

Gelet op

Artikel 7:611 en 7:660 van het Burgerlijk Wetboek

De Wet Bescherming Persoonsgegevens

Artikel 27 lid 1 sub k en I Wet op de ondernemingsraden

Overwegende dat

De OGV&O en haar werknemers zich ten opzichte van elkaar dienen te gedragen als een goed werkgever en een goed werknemer (art. 7:611 BW).

Het gebruik van internet en e-mail voor (veel van) de werknemers binnen Onderwijsgemeenschap Venlo & Omstreken noodzakelijk is om hun werk goed te kunnen doen.

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 werknemers verantwoord gebruik van internet en e-mail wordt verwacht.

Onderwijsgemeenschap Venlo & Omstreken gerechtigd is tot het geven van voorschriften voor gebruik van internet en e-mail en het nemen van maatregelen ter bevordering van de goede orde in de organisatie (artikel 7:660 BW).

De onderhavige gedragscode voorschriften en maatregelen bevat zoals hiervoor genoemd.

Onderwijsgemeenschap Venlo & Omstreken gerechtigd is persoonsgegevens te verwerken ten behoeve van de controle op de naleving van deze gedragscode.

Onderwijsgemeenschap Venlo & Omstreken 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 Gemeenschappelijke Medezeggenschapsraad de volgende gedragscode vastgesteld.

### **1. Werkingssfeer**

Deze regeling is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens van personen in dienst van of werkzaam voor Onderwijsgemeenschap Venlo & Omstreken.

### **2. Uitgangspunten**

- 2.1 De controle op persoonsgegevens over e-mail en internetgebruik is een verwerking van persoonsgegevens in de zin van de Wet Bescherming Persoonsgegevens.
- 2.2 De controle op e-mail- en internetgebruik binnen OGV&O zal conform deze regeling worden uitgevoerd. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het arbeidsrechtelijk kader en de WBP en in overleg met de Gemeenschappelijke Medezeggenschapsraad gehandeld worden.
- 2.3 Gestreefd wordt naar een goede balans tussen verantwoord e-mail- en internetgebruik en bescherming van de privacy van werknemers op de werkplek.
- 2.4 Persoonsgegevens over e-mail en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 6 maanden.
- 2.5 De werkgever treft voorzieningen over de positie en integriteit van de netwerkbeheerders en/of afdeling ICT en de controle daarop.

### **3. Doel**

- 3.1 Deze gedragscode bevat regels ten aanzien van verantwoord e-mail- en internetgebruik en over de wijze waarop controle op persoonsgegevens over e-mail- en internetgebruik plaatsvindt.
- 3.2 De controle op persoonsgegevens over e-mail en internetgebruik vindt plaats met als doel:
  - a. Begeleiding / individuele beoordeling
  - b. Voorkomen van negatieve publiciteit
  - c. Tegengaan van seksuele intimidatie
  - d. Controle op bedrijfsgeheimen
  - e. Systeem en netwerkbeveiliging
  - f. Kosten en capaciteitsbeheersing
  - g. Tegengaan van discriminatie
  - h. Handelingen in strijd met het auteursrecht

### **4. E-mailgebruik**

- 4.1 Het e-mail systeem wordt aan de werknemer voor zakelijk gebruik beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit de functie.
- 4.2 Beperkt persoonlijk gebruik van het e-mailsysteem is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik in de zin van artikel 5 oplevert.

### **5. Verboden e-mailgebruik**

- 5.1 Het is de werknemer niet toegestaan om het e-mailsysteem te gebruiken voor het verzenden van berichten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud.
- 5.2 Het is de werknemer niet toegestaan om het e-mailsysteem te gebruiken voor het verzenden van berichten met een (seksueel) intimiderende inhoud.
- 5.3 Het is de werknemer niet toegestaan om het e-mail systeem te gebruiken voor het verzenden van berichten die (kunnen) aanzetten tot haat en/of geweld.
- 5.4 Het is de werknemer niet toegestaan om het e-mail systeem te gebruiken voor het verzenden van berichten die inbreuk maken op het auteursrecht..

### **6. Internetgebruik**

- 6.1 Internetsysteem wordt aan de werknemer voor zakelijk gebruik beschikbaar gesteld. Gebruik is derhalve verbonden met taken die voortvloeien uit de functie.
- 6.2 Beperkt persoonlijk gebruik van het internet is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik in de zin van artikel 7 oplevert.

### **7. Verboden internetgebruik**

- 7.1 Het is de werknemer niet toegestaan om op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten. Noch is het toegestaan dergelijk materiaal te downloaden
- 7.2 Het is de werknemer niet toegestaan om op internet sites te bezoeken die inbreuk maken op het auteursrecht. Noch is het toegestaan dergelijk materiaal te downloaden.
- 7.3 Het is de werknemer niet toegestaan om op internet sites te bezoeken voor online gokken. Noch is het toegestaan dergelijk materiaal te downloaden.
- 7.4 Het is de werknemer niet toegestaan om zich ongeoorloofd toegang tot niet openbare bronnen op internet te verschaffen.

### **8. Voorwaarden voor controle**

- 8.1 Controle van persoonsgegevens over e-mail- en internetgebruik vindt slechts plaats in het kader van de in artikel 3.2 genoemde doelen.
- 8.2 Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
- 8.3 Indien een werknemer of een groep werknemers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.
- 8.3 Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.

- 8.4 Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Overige controle vindt slechts steekproefsgewijs plaats.
- 8.5 Bij constatering van verboden gebruik wordt dit onmiddellijk met de betrokken werknemer besproken. De werknemer wordt gewezen op de consequenties wanneer hij niet stopt met het verboden gebruik.
- 8.6 E-mailberichten van leden van de GMR 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.

### **9. Controle**

- 9.1 De controle in het kader van begeleiding en/of individuele beoordeling vindt steekproefsgewijs plaats.
- 9.2 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. Verdachte berichten worden automatisch teruggestuurd naar de afzender.
- 9.3 De controle op het uitlekken van bedrijfsgeheimen vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.
- 9.4 De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens.
- 9.5 De controle vindt plaats door de afdeling ICT onder verantwoordelijkheid van het hoofd ICT. Deze verantwoordelijke wijst één of meerdere netwerkbeheerders 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.
- 9.6 Door de verantwoordelijke worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- 9.7 Door de verantwoordelijke worden passende technische en organisatorische maatregelen ten uitvoer gelegd om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

### **10. Vastlegging**

- 10.1 Elektronisch vastleggen van persoonsgegevens geschiedt (automatisch) door de door de OGV&O ingezette software.
- 10.2 De vastlegging beperkt zich tot de gegevens die noodzakelijk zijn voor de doeleinden van de verwerking, te weten:
- voor het verkrijgen van inzicht in de mate van gebruik van de elektronische communicatiemiddelen worden alleen stroom- en soortgegevens vastgelegd;

- voor het voorkomen van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen wordt het gebruik van de elektronische communicatiemiddelen op individueel en inhoudelijk niveau gevolgd. Dit geschiedt slechts bij een redelijk vermoeden van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen.

### **11. Persoonsgegevens**

- 11.1 In de in artikel 7 genoemde vastlegging worden ten hoogste de volgende persoonsgegevens opgenomen:
- a) gebruikersidentificatie, naam, voornaam of voorletters van de betrokkene;
  - b) naam en/of codering van de campus cq sector cq afdeling waaronder de betrokkene valt;
  - c) gegevens over de toegang tot internet die door de OGV&O is geboden aan de betrokkene, 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 emailberichten 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) Bij zwaarwegende redenen kan ook overgegaan worden tot vastlegging van:
  - g) de inhoud van de door de betrokkene verzonden, dan wel ontvangen emailberichten.
- 11.2 Indien er een redelijk vermoeden bestaat van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen door betrokkene, kan door de verantwoordelijke opdracht worden gegeven om de in het eerste lid, sub e en/of f van dit artikel bedoelde, gegevens vast te leggen en te verstrekken aan de personen bedoeld in artikel .

### **12. Bewaring en verwijdering**

- 12.1 De in artikel 11, eerste lid, genoemde 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.
- 12.2 Indien de afdeling ICT om technische redenen persoonsgegevens als bedoeld in artikel 11, eerste lid, niet kan verwijderen, wordt onder verwijderen verstaan het niet meer verstrekken van deze gegevens voor de in artikel 3 geformuleerde doeleinden.

### **13. Personen aan wie persoonsgegevens worden verstrekt**

De vastgelegde persoonsgegevens worden, na bewerking, verstrekt aan:

- 13.1 Het teamcoördinator ICT om inzicht te verkrijgen in de mate van gebruik van de elektronische communicatiemiddelen.
- 13.2 De concerncontroller indien er een redelijk vermoeden bestaat van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen. Het betreft hier dan de gegevens als bedoeld in artikel 8;
- 13.3 Degene(n) die op verzoek van de werkgever is (zijn) belast met of leiding geeft (geven) aan onderzoek naar onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen. Het betreft hier dan de gegevens als bedoeld in artikel 8.

**14. Rechten van de werknemer**

- 14.1 Onderwijsgemeenschap Venlo & Omstreken informeert de werknemer voorafgaand aan de controle op persoonsgegevens over e-mail en internetgebruik, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.
- 14.2 De werknemer kan zich tot Onderwijsgemeenschap Venlo & Omstreken wenden met het verzoek voor een volledig overzicht van zijn bewerkte persoonsgegevens. Het verzoek wordt binnen 4 weken beantwoord.
- 14.3 De werknemer kan de Onderwijsgemeenschap Venlo & Omstreken verzoeken zijn 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 zijn, dan wel in strijd met een wettelijk voorschrift zijn. Het verzoek wordt binnen 4 weken beantwoord.

Werknemer is en blijft verantwoordelijk voor de per email ontvangen bedrijfsinformatie en al dan niet digitale archivering daarvan (backup uitgezonderd). In principe dient email behandeld te worden als normale inkomende en uitgaande post

**15. Slotbepaling**

Onderwijsgemeenschap Venlo & Omstreken kan deze gedragscode met instemming van de Gemeenschappelijke Medezeggenschapsraad wijzigen of intrekken.



## HOOFDSTUK 1 DEFINITIES, REIKWIJDTE EN DOELEINDEN

### Artikel 1 Definities

In dit reglement wordt verstaan onder :

1. Wbp: Wet bescherming persoonsgegevens.
2. College bescherming persoonsgegevens: het College als bedoeld in artikel 51 Wbp.
3. OGV&O: De Samenwerkingsstichting Voortgezet Onderwijs Regio Venlo (hoden Onderwijsgemeenschap Venlo & Omstreken)
4. Betrokkene: gebruiker van de elektronische communicatiemiddelen op wie een persoonsgegeven betrekking heeft en die aan te merken is als :
  - a. medewerker in dienst van de OGV&O;
  - b. persoon die (betaalde of niet-betaalde) werkzaamheden voor de OGV&O verricht, anders dan in arbeidsrechtelijk dienstverband.
5. Emailfaciliteiten: de door of namens de OGV&O aan betrokkenen ter beschikking gestelde emailfaciliteiten.
6. Internetfaciliteiten: de door of namens de OGV&O aan betrokkenen ter beschikking gestelde internetfaciliteiten.
7. Elektronische communicatiemiddelen: email- en/of internetfaciliteiten.
8. Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van de Wbp.
9. Verwerken van persoonsgegevens: elke handeling of 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.
10. Bestand: elk, al dan niet geautomatiseerd, gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.
11. Verantwoordelijke: het College van Bestuur, zijnde het bestuursorgaan dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
12. Onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen: een doen of nalaten in strijd met dit privacyreglement of andere wet- en regelgeving of een inbreuk op een recht.

### Artikel 2 Reikwijdte

1. Dit privacyreglement is van toepassing op het verwerken van persoonsgegevens inzake het gebruik van elektronische communicatiemiddelen.
2. Dit privacyreglement geldt voor medewerkers in dienst van de OGV&O en personen die (betaalde of niet-betaalde) werkzaamheden voor de OGV&O verrichten, anders dan in arbeidsrechtelijk dienstverband.

### Artikel 3 Doeleinden

1. De verwerking van persoonsgegevens inzake het gebruik van de elektronische communicatiemiddelen heeft de volgende doeleinden:
  - a. het verkrijgen van inzicht in de mate van gebruik van de elektronische communicatiemiddelen;
  - b. het voorkomen van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen.
2. De omvang van de controle ter voorkoming van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen als bedoeld in het eerste lid sub b, wordt zo beperkt mogelijk gehouden, in die zin dat deze in redelijke verhouding staat tot het doel waarvoor deze wordt aangewend.

## HOOFDSTUK 2 VERANTWOORDELIJKHEDEN EN BEHEER

### Artikel 4 Verantwoordelijkheden en beheer

1. Door de verantwoordelijke worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
2. Door de verantwoordelijke worden passende technische en organisatorische maatregelen ten uitvoer gelegd om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
3. Door de verantwoordelijke worden één of meerdere netwerk- cq systeembeheerders aangewezen 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.

## HOOFDSTUK 3 GEBRUIK ELEKTRONISCHE COMMUNICATIEMIDDELEN

### Artikel 5 Gebruik elektronische communicatiemiddelen

1. Betrokkenen gebruiken de elektronische communicatiemiddelen primair voor het uitvoeren van de aan hen door de OGV&O opgedragen taken.
2. Incidenteel privé-gebruik van de elektronische communicatiemiddelen door betrokkenen is toegestaan mits dit gebruik in overeenstemming is met dit privacyreglement en dit gebruik in geen geval storend is voor dan wel ten koste gaat van het uitvoeren van de aan hen door de OGV&O opgedragen taken.
3. Het is betrokkenen niet toegestaan met behulp van de emailfaciliteiten kettingbrieven te versturen of pornografisch materiaal te versturen of op te vragen, dan wel dreigende, seksueel intimiderende, racistische of discriminerende opmerkingen te maken. Evenmin is het betrokkenen toegestaan zonder voorafgaand overleg met de systeembeheerder(s) met behulp van de emailfaciliteiten software te verzenden of op te vragen waarvan betrokkene redelijkerwijs moet aannemen dat deze te omvangrijk zijn.
4. Het is betrokkenen niet toegestaan met behulp van de internetfaciliteiten bewust internetsites die pornografisch, dan wel racistisch materiaal bevatten te bezoeken, mee te doen in privé chatsessies, online te gokken, downloaden van bestanden waarop copyright rust en zonder voorafgaand overleg met de systeembeheerder(s) software te downloaden waarvan betrokkene redelijkerwijs moet aannemen dat deze te omvangrijk zijn.
5. Zonder voorafgaande toestemming van het bestuur cq de manager is het betrokkenen niet toegestaan met behulp van de emailfaciliteiten een elektronisch bericht aan alle of vrijwel alle medewerkers van de OGV&O tegelijkertijd te versturen.
6. Indien betrokkenen met gebruik van de internetfaciliteiten handelingen verrichten die als emailtoepassingen zijn te kwalificeren, dan zijn de bepalingen van artikel 5, derde en vijfde lid, van overeenkomstige toepassing.
7. Betrokkenen zullen bij het gebruik van de elektronische communicatiemiddelen de nodige zorgvuldigheid betrachten en de integriteit en goede naam van de OGV&O waarborgen.
8. Het doen van bestellingen met behulp van internet is en blijft voorbehouden aan daartoe geautoriseerde personen cq. afdelingen.

### Artikel 6 Voorkomen onrechtmatig gebruik dan wel misbruik

De OGV&O neemt zo veel mogelijk maatregelen in technische zin ter voorkoming van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen.

## HOOFDSTUK 4 VASTLEGGING, BEWARING, VERWIJDERING EN VERSTREKKING PERSOONSGEGEVENS

### Artikel 7 Vastlegging

1. Elektronisch vastleggen van persoonsgegevens geschiedt (automatisch) door de door de OGV&O ingezette software.
2. De vastlegging beperkt zich tot de gegevens die noodzakelijk zijn voor de doeleinden van de verwerking als bedoeld in artikel 3, te weten:
  - a. voor het verkrijgen van inzicht in de mate van gebruik van de elektronische communicatiemiddelen worden alleen stroom- en soortgegevens vastgelegd;
  - b. voor het voorkomen van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen wordt het gebruik van de elektronische communicatiemiddelen op individueel en inhoudelijk niveau gevolgd. Dit geschiedt slechts bij een redelijk vermoeden van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen.

### Artikel 8 Persoonsgegevens

- 1) In de in artikel 7 genoemde vastlegging worden ten hoogste de volgende persoonsgegevens opgenomen:
  - a) gebruikersidentificatie, naam, voornaam of voorletters van de betrokkene;
  - b) naam en/of codering van de campus cq sector cq afdeling waaronder de betrokkene valt;
  - c) gegevens over de toegang tot internet die door de OGV&O is geboden aan de betrokkene, 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 emailberichten 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;Bij zwaarwegende redenen kan ook overgegaan worden tot vastlegging van:
  - f) de inhoud van de door de betrokkene verzonden, dan wel ontvangen emailberichten.
- 2) Indien er een redelijk vermoeden bestaat van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen door betrokkene, kan door de verantwoordelijke opdracht worden gegeven om de in het eerste lid, sub e en/of f van dit artikel bedoelde, gegevens vast te leggen en te verstrekken aan de personen bedoeld in artikel 10.
- 3) In principe zijn emailberichten aan MR-leden, bedrijfsartsen en andere nadere vast te leggen personen uitgesloten van controle. Dit geldt niet voor veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.

### Artikel 9 Bewaring en verwijdering

1. De in artikel 8, eerste lid, genoemde 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.
2. Indien de systeembeheerder om technische redenen persoonsgegevens als bedoeld in artikel 9, eerste lid, niet kan verwijderen, wordt onder verwijderen verstaan het niet meer verstrekken van deze gegevens voor de in artikel 3 geformuleerde doeleinden.

**Artikel 10 Personen aan wie persoonsgegevens worden verstrekt**

De vastgelegde persoonsgegevens worden, na bewerking, verstrekt aan:

1. Het afdelingshoofd ICT om inzicht te verkrijgen in de mate van gebruik van de elektronische communicatiemiddelen. Het betreft hier dan slechts de gegevens als bedoeld in artikel 8, eerste lid, sub a tot en met d in geaggregeerde, niet tot de persoon herleidbare vorm;
2. De concerncontroller indien er een redelijk vermoeden bestaat van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen. Het betreft hier dan de gegevens als bedoeld in artikel 8, eerste lid;
3. Degene(n) die op verzoek van de verantwoordelijke is (zijn) belast met of leiding geeft (geven) aan onderzoek naar onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen. Het betreft hier dan de gegevens als bedoeld in artikel 8, eerste lid.

## **HOOFDSTUK 5 RECHTEN VAN BETROKKENE: VERBETEREN, AANVULLEN, VERWIJDEREN OF AFSCHERMEN PERSOONSGEGEVENS**

### **Artikel 11 Rechten en plichten van de betrokkene**

- 1) Aan de betrokkene die daarom aan verantwoordelijke verzoekt, wordt een overzicht verschaft van de hem / haar betreffende persoonsgegevens die worden verwerkt. Indien een gewichtig belang van de verzoeker dit eist, voldoet de verantwoordelijke aan dit verzoek in een andere dan schriftelijke vorm, die aan dat belang is aangepast. Het verzoek wordt binnen 4 weken na ontvangst van het verzoek beantwoord.
- 2) Degene aan wie overeenkomstig het eerste lid kennis is gegeven van de hem/haar betreffende persoonsgegevens, kan de verantwoordelijke verzoeken deze te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk 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 worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen en wordt binnen 4 weken na ontvangst van het verzoek beantwoord.
- 3) De werknemer kan bij de werkgever verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. De werkgever oordeelt binnen 4 weken na ontvangst van het verzet of dit gerechtvaardigd is. Zo ja wordt de verwerking terstond beëindigd.
- 4) De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het in het eerste, tweede en derde lid genoemde verzoek schriftelijk of, dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed.
- 5) De verantwoordelijke draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.
- 6) Werknemer is en blijft verantwoordelijk voor de per email ontvangen bedrijfsinformatie en al dan niet digitale archivering daarvan (backup uitgezonderd). In principe dient email behandeld te worden als normale inkomende en uitgaande post.

## HOOFDSTUK 6 SOCIAL MEDIA

### Het gebruik van sociale media tijdens werktijd

#### Artikel 12

- 1) Medewerkers mogen in werktijd gebruikmaken van sociale netwerken, voor zover dat niet ten koste gaat van werk en verantwoordelijkheden. Afhankelijk van de functie kan het gebruik van sociale media tijdens werktijd meer of minder gewenst zijn. De leidinggevende maakt hierover afspraken met zijn of haar medewerkers.
- 2) De medewerker blijft zelf verantwoordelijk voor wat hij / zij communiceert, onder welke naam of alias hij / zij dat ook doet.
- 3) Medewerkers gaan in principe geen virtuele “vriendschappen” aan met leerlingen. Voor vriendschappen met pedagogische doeleinden dient goedkeuring gevraagd te worden aan het management. Uitzonderingen zijn directe familierelaties.
- 4) Medewerkers mogen geen accounts of aliassen aanmaken zonder toestemming van het College van Bestuur en / of de campusdirectie, indien de Onderwijsgemeenschap Venlo & Omstreken of een van de campussen op enigerlei wijze deel uitmaken van die accountnaam of alias.
- 5) Foto-, film- en geluidsopnamen van schoolgerelateerde zaken mogen niet op sociale media geplaatst worden, tenzij de betrokkenen hier uitdrukkelijk toestemming voor hebben gegeven.
- 6) Als een medewerker op sociale media dingen doet / zegt die schadelijk zijn voor Onderwijsgemeenschap Venlo & Omstreken en / of een van de campussen wordt hij / zij door zijn / haar leidinggevende daar op aangesproken.
- 7) Als een medewerker iets communiceert dat direct of indirect betrekking heeft op Onderwijsgemeenschap Venlo & Omstreken en / of een van de campussen, dan wordt hij / zij geacht zich niet negatief over de organisatie uit te laten.
- 8) Als een medewerker iets communiceert dat direct of indirect gaat over Onderwijsgemeenschap Venlo & Omstreken en / of een van de campussen dan is het hem / haar niet toegestaan dit te doen *namens* de Onderwijsgemeenschap. Communicatie namens Onderwijsgemeenschap Venlo & Omstreken en / of de campussen verloopt altijd via het officiële account.
- 9) Medewerkers moeten kritisch zijn met het reageren op fora, groepen en discussies die betrekking hebben op hun specifieke werkveld. In geval van een onplezierige discussie: stop ermee.
- 10) Medewerkers moeten er rekening mee houden dat ze in de communicatie geen informatie verspreiden over derden die daar geen toestemming voor hebben gegeven, met name ook leerlingen. Steeds meer toepassingen (zoals Foursquare, maar ook bijvoorbeeld Twitter) sturen een locatie mee en maken deze beschikbaar voor derden, waardoor iemand dus ook informatie over derden onbedoeld kan communiceren.
- 11) Medewerkers dienen weloverwogen te reageren. Het is aan te raden twee keer na te denken voordat een post gedaan wordt. Medewerkers doen online niets wat offline ook niet kan. De medewerker is zelf verantwoordelijk voor zijn handelingen.

## HOOFDSTUK 7 Gebruik van ICTmiddelen die eigendom zijn van de OGVO

### Artikel 13

- 1) Het is medewerkers niet toegestaan ICTapparatuur die eigendom van de OGVO is te modificeren tenzij daar uitdrukkelijk toestemming voor is verleend door het CvB. Hierbij moet bijvoorbeeld gedacht worden aan het zogenaamde jailbreaken van Appleapparatuur (iDevices).



## HOOFDSTUK 8 SANCTIES, OPENBAARMAKING, INWERKINGTREDING EN SLOTBEPALING

### **Artikel 14 Sancties**

Overtreders van dit privacyreglement worden door de leidinggevende zo spoedig mogelijk aangesproken. Afhankelijk van de duur, ernst en recidive kan dit voor medewerkers in dienst van de OGV&O resulteren in disciplinaire maatregelen als bedoeld in de arbeidsvoorwaardenregeling van de OGV&O.

Overtreding van dit privacyreglement kan voor personen die (betaalde of niet-betaalde) werkzaamheden voor de OGV&O verrichten, anders dan in arbeidsrechtelijk dienstverband, resulteren in maatregelen waardoor deze personen, al dan niet tijdelijk, geen beschikking meer hebben over (een deel van) de elektronische communicatiemiddelen of een beëindiging van de werkzaamheden betekenen.

### **Artikel 15 Onvoorziene omstandigheden**

In gevallen waarin dit privacyreglement niet voorziet of bij twijfel omtrent de toepassing van dit privacyreglement beslist het College van Bestuur.

### **Artikel 16 Openbaarmaking en inwerkingtreding**

Dit privacyreglement wordt verstrekt of ter beschikking gesteld aan degenen die, direct of indirect, de beschikking krijgen over elektronische communicatiemiddelen.

Dit privacyreglement treedt in werking op 1 april 2005 en wordt jaarlijks geactualiseerd.

### **Artikel 17 Slotbepaling**

- 1) Het College van Bestuur kan dit reglement wijzigen met instemming van de GMR. De wijzigingen worden schriftelijk vastgelegd en ter kennisname gebracht aan de medewerkers (zie ook artikel 14).
- 2) Onverminderd het bepaalde in dit privacyreglement, zal op het verwerken van persoonsgegevens de op 1 september 2001 in werking getreden Wbp van toepassing zijn. Deze regeling wordt jaarlijks geëvalueerd.