



# GEDRAGSCODE ICT

Uitgave	: ROC van Amsterdam / ROC van Flevoland
Auteur	: S. Ritzen, Juridische Zaken
Kenmerk	: Gedragscode ICT
Vastgesteld door CvB ROCvA op	: 30-06-2014
Beschikbaar voor OR ROCvA op	: ter informatie d.d. 04-07-2014
Beschikbaar voor CSR ROCvA op	: ter informatie d.d. 04-07-2014
Beschikbaar voor GMR VOvA op	: ter informatie d.d. 04-07-2014
Vastgesteld door CvB ROCvF op	: 30-06-2014
Beschikbaar voor OR ROCvF op	: ter informatie d.d. 04-07-2014
Beschikbaar voor CSR ROCvF op	: ter informatie d.d. 04-07-2014

# Inhoudsopgave

	<b>Inleiding</b>	<b>03</b>
<b>1.</b>	<b><u>Algemene bepalingen</u></b>	<b>04</b>
1.	Reikwijdte	04
2.	Doel	04
3.	Aard Gedragscode ICT	04
4.	Aanspreekbaarheid	04
<b>2.</b>	<b><u>Omgaan met accountgegevens</u></b>	<b>05</b>
1.	Ter beschikking stellen van gebruikersaccount	05
2.	Ter beschikking stellen van emailadres	05
3.	Wachtwoord	05
4.	Digipass	05
<b>3.</b>	<b><u>ICT Faciliteiten</u></b>	<b>06</b>
1.	Professioneel en integer handelen	06
2.	Richtlijnen m.b.t. A t/m D	06
A.	<u>Computers</u>	06
1	Geoorloofd gebruik	06
2.	Opslag bestanden	06
B.	<u>Internet</u>	07
1.	Aanstootgevende websites	07
2.	Verboden online activiteiten	07
C.	<u>Email</u>	07
1.	Taalgebruik	07
D.	<u>Mobiele communicatiemiddelen</u>	08
1.	Gebruik Smartphones, smartwatches, tablets	08
<b>4.</b>	<b><u>Social media</u></b>	<b>09</b>
1.	Officiële social media kanalen van de organisatie	09
2.	Persoonlijke social media kanalen	09
3.	Maken en/of publiceren van beeld- of geluidsopnames	10
<b>5.</b>	<b><u>Schending Gedragscode ICT</u></b>	<b>11</b>
1.	Naleving Gedragscode ICT	11
2.	Inhoudelijke controle gebruik ICT faciliteiten	11
3.	Procedure	11
4.	Disciplinaire maatregelen	11
<b>6.</b>	<b><u>Slotbepalingen</u></b>	<b>12</b>
1.	Vaststellingstraject	12
2.	Inwerkingtreding en duur reglement	12
	<b>Bijlage:</b>	
<b>1.</b>	<b><u>Begrippenlijst</u></b>	<b>14</b>

## **Inleiding**

Het ROC van Amsterdam, het Voortgezet Onderwijs van Amsterdam en het ROC van Flevoland (hierna: de Organisatie”) hebben 5 jaar geleden hun krachten gebundeld en zijn hiermee een van de grootste aanbieders in Nederland op het gebied van vmbo en mbo onderwijs geworden. Samen bieden zij onderwijs aan duizenden vmbo en mbo studenten en werk aan duizenden werknemers, afkomstig uit diverse culturen en sociale geledingen. De omvang en de verscheidenheid van mensen die samen de organisatie vormen, stellen eisen aan de manier waarop binnen de organisatie met elkaar wordt omgegaan.

Als medewerker en student van de organisatie maak je gebruik van de ICT-faciliteiten die de school aanbiedt. Aan dit gebruik zitten een aantal regels vast, waar zowel de organisatie als iedere gebruiker zich aan dient te houden.

In de loop der jaren zijn de mogelijkheden op ICT gebied verveelvoudigd en zijn de regels daaromtrent complex geworden. De organisatie stelt niet meer alleen computers op het werk beschikbaar, maar krijgt nu te maken met zaken als: draadloos netwerk (Wi-Fi), nieuwe softwarepakketten, een nieuwe communicatie-omgeving (e-mail, SharePoint, Lync), internet. Daarnaast stelt het aan medewerkers smartphones, tablets, laptops en andere mobile devices ter beschikking. Ook de vraag hoe wij als school en werkgever willen omgaan en gebruik maken van social media is een actueel thema geworden.

In deze Gedragscode ICT leggen wij vast wat de randvoorwaarden zijn voor onze organisatie. Wij behandelen elkaar met respect, gaan zorgvuldig met onze gegevens om en die van een ander en respecteren elkaars privacy. Onze organisatie kan alleen goed functioneren indien zij een stevige basis kent die breed door de medewerkers gedragen wordt. Wij hopen dat deze Gedragscode ICT een waardevolle aanvulling kan zijn op deze fundering.

### **ROC van Amsterdam**

De heer drs. E.C.M. de Jaeger  
Voorzitter College van Bestuur

### **Voortgezet Onderwijs van Amsterdam**

De heer R.J.W. Winter  
Gedelegeerd bestuurder

### **ROC van Flevoland**

De heer R.C.A. Wilcke  
Voorzitter College van Bestuur

# 1. Algemene bepalingen

## 1. Reikwijdte

1. Deze Gedragscode ICT is van toepassing op alle gebruikers.
2. Gebruikers zijn:
  - Werknemers, uitzendkrachten, ZZP-ers, gastdocenten, vrijwilligers, stagiaires en alle anderen die in opdracht van de organisatie werkzaamheden verrichten.
  - Studenten van de organisatie.
  - Iedereen aan wie door de organisatie:
    - een gebruikersaccount is verstrekt.
    - toestemming is gegeven tot gebruikmaking van ICT faciliteiten.
2. In deze Gedragscode ICT wil de organisatie met een aantal richtlijnen gewenst en ongewenst gedrag vastleggen op ICT gebied in de ruimste zin des woords en houvast bieden bij het maken van de juiste keuzes.

## 2. Doel

Het doel van deze Gedragscode ICT is het stellen van regels over het verantwoord gebruik van internet, sociale media en e-mail door gebruikers aan wie door de organisatie voor zakelijke doeleinden ICT faciliteiten ter beschikking zijn gesteld.

## 3. Aard Gedragscode ICT

1. De Gedragscode ICT is opgesteld om een duurzaam en flexibel document te zijn dat jarenlang kan blijven gelden zonder steeds te hoeven worden gewijzigd. De gedragscode ICT maakt een integraal onderdeel uit van de Integriteitscode van de organisatie.
2. De Gedragscode ICT geeft algemene richtlijnen, de uitwerking van deze richtlijnen wordt vastgelegd in het beleidsdocument "Gedragsregels ICT".
3. Voor details en informatie over de in de Gedragscode ICT genoemde richtlijnen kan men de website raadplegen of de Servicedesk bellen.
4. Definities zijn te raadplegen in bijlage 1 bij deze Gedragscode ICT.

## 4. Aanspreekbaarheid

1. In de Gedragscode ICT staat aangegeven wat van gebruikers wordt verwacht om het werken en studeren binnen onze organisatie prettig en succesvol te laten verlopen.
2. Elke gebruiker wordt geacht de inhoud van de Gedragscode ICT te kennen en zich hier aan te houden.
3. Gebruikers zijn te allen tijde aanspreekbaar op het naleven van de Gedragscode ICT.
4. De Gedragscode ICT is door iedereen in te zien op de website van de organisatie.

## **2. Omgaan met accountgegevens**

### **1. Ter beschikking stellen van gebruikersaccount**

1. Voor iedere gebruiker wordt door de Dienst ICT een gebruikersaccount aangemaakt waardoor men gebruik kan maken van de ICT-faciliteiten.
2. Om gebruik te kunnen maken van de ICT-faciliteiten moet een persoonlijk wachtwoord gekozen worden. Dit wachtwoord dient gebruiker periodiek te wijzigen.
3. Het aan derden ter beschikking stellen, op welke wijze dan ook, van persoonlijke accountgegevens is niet toegestaan.
4. Van de gebruiker van de accountgegevens wordt verwacht dat hij maatregelen treft om te voorkomen dat personen zijn wachtwoord kunnen achterhalen en zijn account kunnen misbruiken.
5. De gebruiker van de accountgegevens blijft verantwoordelijk voor het gebruik dat gemaakt wordt van de accountgegevens, inclusief alle schade die hieruit kan voortvloeien.

### **2. Ter beschikking stellen van emailadres**

1. Iedere gebruiker krijgt een persoonlijk e-mailaccount van de organisatie. Dit geldt zowel voor medewerkers als studenten.
2. Voor het ROCvA geldt als emailaccount het volgende:
  - Studenten van ROCvA krijgen bijvoorbeeld een account bestaand uit **voornaam.achternaam@student.rocva.nl**.
  - Medewerkers van ROCvA krijgen bijvoorbeeld een account bestaand uit **voorletter.achternaam@rocva.nl**.
3. Gebruikers van ROCvF en VOvA krijgen respectievelijk een ROCvF of VOvA extensie.
4. Gebruikers dienen het aan hen toegekende emailadres te gebruiken bij correspondentie wegens werk dan wel studie.
5. De emailaccount van de gebruiker heeft een ruime opslagcapaciteit, waardoor de kans dat mails niet ontvangen kunnen worden gering is.

### **3. Wachtwoord**

1. De gebruiker is vrij in de keuze van een persoonlijk wachtwoord.
2. De organisatie verzoekt gebruikers zorgvuldig te werk te gaan bij de keuze van een wachtwoord en een wachtwoord te kiezen dat men goed kan onthouden, maar dat niet snel is te achterhalen.
3. Indien een gebruiker de indruk heeft dat zijn wachtwoord bekend is geworden of dat hij van mening is dat zijn account is gehackt, dient hij direct de Servicedesk van de organisatie in te schakelen.
4. Gebruiker dient bij het uitlekken van zijn wachtwoord onmiddellijk zijn wachtwoord te wijzigen.
5. Voor adviezen over het kiezen van een wachtwoord kan men de Gedragsregels ICT raadplegen.
6. Medewerkers van de Servicedesk zullen gebruiker nimmer naar hun wachtwoord vragen. Indien dit toch is gebeurd, dient de gebruiker zijn wachtwoord te wijzigen.

### **4. Digipass**

1. Medewerkers krijgen een persoonlijke digipass van de organisatie waardoor men gebruik kan maken van kernapplicaties (bijvoorbeeld EduArte). Het beveiligen van kernapplicaties is nodig om bijvoorbeeld examenfraude binnen de organisatie, te voorkomen.
2. Om gebruik te kunnen maken van de kernapplicatie moet de persoonlijke digipass worden geactiveerd en voorzien worden van een persoonlijke pincode.
3. Het aan derden ter beschikking stellen, op welke wijze dan ook, van een persoonlijke digipass is niet toegestaan.
4. De gebruiker van de digipass blijft verantwoordelijk voor het gebruik en is aansprakelijk voor alle schade die hieruit kan voortvloeien.
5. Van de gebruiker van de digipass wordt verwacht dat hij maatregelen treft om te voorkomen dat andere personen zijn persoonlijke pincode kunnen achterhalen en zijn digipass kunnen misbruiken.

### **3. ICT Faciliteiten**

Het recht op gebruikmaking van ICT faciliteiten van de organisatie wordt begrensd door de redelijkheid en billijkheid die partijen tegenover elkaar in acht dienen te nemen. Gebruik ervan is noodzakelijk maar ongeoorloofd gebruik kan leiden tot onnodige risico's en schade. Ongeoorloofd gebruik kan vele vormen aannemen die zich niet in een gedragscode laten vangen.

Een gulden middenweg waarbij de kaders goed zijn omschreven is dan ook onontbeerlijk. De organisatie geeft hieronder richtlijnen voor gewenst en ongewenst gedrag zodat het duidelijk is wat partijen van elkaar mogen verwachten.

#### **1. Professioneel en integer handelen**

1. De organisatie verlangt van haar gebruikers dat zij professioneel en integer handelen bij het gebruik van de ICT faciliteiten.
2. Gebruikers dienen zich bij het gebruik van de ICT-faciliteiten tevens te houden aan de Nederlandse wet- en regelgeving.
3. Onder ICT faciliteiten wordt in deze gedragscode ICT verstaan:
  - A. Computers
  - B. Internet
  - C. Email
  - D. Mobiele communicatiemiddelen
4. Professionaliteit uit zich in gebruik maken van de faciliteiten voor het doel waarvoor het is gegeven. Integer gedrag uit zich onder meer in het niet onnodig risico's creëren en een open en duidelijke communicatie naar elkaar, waarbij respect voor elkaar voorop staat.

#### **A. COMPUTERS**

##### **1. Geoorloofd gebruik**

1. De organisatie stelt aan haar medewerkers een werkruimte en computer beschikbaar, mits dit voor hun functie noodzakelijk is.
2. De organisatie bezit op diverse locaties computers waarvan studenten gebruik kunnen maken indien de les dit vereist. Daarnaast hebben veel locaties van de organisatie zogeheten open leercentra (OLC's) en/of studieruimtes waar men gebruik mag maken van aldaar aanwezige computers.
3. Een gebruiker gebruikt de computer hoofdzakelijk voor zakelijke gebruik danwel voor studie.
4. Gebruik voor zaken in de privésfeer is binnen redelijke grenzen toegestaan. Privégebruik mag nooit storend zijn voor de goede voortgang van de dagelijkse werkzaamheden.
5. Van gebruiker wordt verwacht dat hij zijn computer lockt als hij tijdelijk zijn werkplek of locatie verlaat.
6. Indien gebruiker gebruik maakt van zijn privé PC, laptop of tablet dient deze voorzien te zijn van een anti virusprogramma en een firewall. Tevens dienen de door de leverancier van het besturingssysteem geadviseerde beveiligingsupdates te zijn geïnstalleerd.
7. Van gebruiker wordt terughoudendheid verwacht bij het openen van ongewenste of onbekende email en van attachments op internet.
8. Verspreiding van computervirussen dient te allen tijde worden voorkomen. Indien gebruiker gewaarschuwd wordt voor een dergelijk virus, dient gebruiker de aanwijzingen van de Dienst ICT op te volgen.

##### **2. Opslag bestanden**

Het opslaan van bestanden is afhankelijk van de computer die men gebruikt. Om onnodig dataverlies te genereren worden hieronder richtlijnen gegeven voor het opslaan van bestanden. De organisatie is niet aansprakelijk voor verlies van bestanden die niet correct zijn opgeslagen bv op het bureaublad of de C schijf.

1. Computer in algemene ruimte  
Indien men gebruik maakt van een computer in de algemene ruimtes binnen de organisatie, dient men de bestanden niet op te slaan op de harde schijf van de computer maar gebruik te maken van externe opslagmedia, zoals bijvoorbeeld de door de Dienst ICT aangeboden opslagmedia (netwerkschijf OneDrive voor bedrijven) of Privé opslagmedia (USB stick, Cloudopslag)
2. Persoonlijk toegewezen computer  
Indien men gebruik maakt van een aan gebruiker persoonlijk toegewezen computer dan dient men bestanden op te slaan op de door de organisatie aangeboden opslagmedia, zoals de netwerkschijf (bv de persoonlijke schijf danwel de afdelingsschijf), OneDrive voor bedrijven (persoonlijk) of SharePoint (afdelings- of samenwerkingschijf).
3. Aan medewerker toegewezen computer  
Het is voor medewerkers mogelijk om bestanden op te slaan in de voor de gebruiker bestemde mappen (afdeling/team, persoonlijk, OneDrive) op de centrale server of in de Cloud.
4. Het opslaan, bekijken of anderszins in bezit hebben van pornografisch en/of kinder pornografische afbeeldingen is verboden en zal tot maatregelen kunnen leiden. Dergelijke bestanden zullen zonder toestemming van de gebruiker kunnen worden verwijderd.

## **B. INTERNET**

### **1. Aanstootgevende websites**

1. Het is gebruikers verboden om websites te bezoeken met aanstootgevende inhoud.
2. Van aanstootgevende inhoud is in ieder geval sprake bij pornografie in de ruimste zin des woords, racisme, haat, geweld en discriminatie.
3. Het is gebruikers niet toegestaan om materiaal in de ruimste zin des woords te publiceren dat in strijd is met de wet of goede zeden.
4. De organisatie behoudt zich het recht voor om toegang tot bepaalde websites te beperken danwel blokkeren. Het feit dat een bepaalde website niet is geblokkeerd, ontslaat Gebruiker niet van de verplichting zich te onthouden van bezoeken van websites met pornografisch, discriminerend, racistische of op entertainment gerichte inhoud.

### **2. Verboden online activiteiten**

1. Het is gebruikers verboden om (illegale) of door de organisatie verboden programma's te installeren of bestanden te downloaden.
2. Indien geconstateerd worden dat een gebruiker de website van De organisatie danwel externe bedrijven heeft gekraakt, gehackt of dit heeft geprobeerd, wordt direct aangifte gedaan bij de politie. De organisatie zal gebruiker volledig aansprakelijk stellen voor alle schade die hieruit voortvloeit. Tevens zal de organisatie alle medewerking verlenen aan politie bij het doen van onderzoek naar de identiteit van gebruiker.
3. Het lastig vallen of pesten van gebruikers via ICT faciliteiten en/of social media is niet toegestaan en zal leiden tot disciplinaire maatregelen.

## **C. EMAIL**

### **1. Taalgebruik**

1. Op taalgebruik in e-mails en overige online communicatie is de integriteitscode van de organisatie integraal van toepassing. Dit betekent dat gebruikers elkaar respectvol zullen aanspreken racistische, seksueel intimiderende, discriminerende of anderszins beledigende uitingen niet zijn toegestaan.
2. Indien een gebruiker aangeeft gepest te worden via de emailaccount van de organisatie, behoudt de organisatie zich het recht voor om een controle op de emailaccount te doen en de inhoud daarvan te controleren.
3. Indien dergelijke bestanden worden aangetroffen kan dit tot disciplinaire maatregelen leiden voor de verzender.
4. Het is gebruikers niet toegestaan om kettingmails, junkmail of spam mail te sturen of door te sturen.

**D. MOBIELE COMMUNICATIEMIDDELEN**

**1. Gebruik mobiele communicatiemiddelen**

1. Onder mobiele communicatiemiddelen worden devices begrepen zoals smartphones, smartwatches, tablets. Deze opsomming is echter niet limitatief gezien de voortschrijding van de technologie.
2. Het gebruik van mobiele communicatiemiddelen is voor medewerkers en studenten toegestaan, mits het gebruik hiervan de werkzaamheden niet verstoort.
3. Gebruik van mobiele communicatiemiddelen (waaronder bellen, sms'en, spelletjes doen etc.) in het leslokaal danwel tijdens de les is niet toegestaan, tenzij het gebruik onderdeel uitmaakt van de les.
4. Studenten zetten hun telefoon op stil tijdens de lessen, tenzij dit met de docent anders is afgesproken. De organisatie behoudt zich het recht voor om gedurende de les mobiele communicatiemiddelen in te nemen bij overtreding van de richtlijnen.



## 4. Social media

Social media zijn een vast onderdeel binnen de samenleving geworden. Ook in het onderwijs wordt steeds meer gebruik gemaakt van de mogelijkheden van social media. Via social media (Twitter, Facebook etc.), netwerken, weblogs, fora en beoordelingsites deelt een groeiend aantal mensen ervaringen met en meningen over de organisatie.

Hoewel de organisatie het gebruik van social media toejuicht beseft zij ook dat zij hierdoor kwetsbaar is. Daarom heeft De organisatie de volgende richtlijnen opgesteld, waar gebruikers zich zowel privé als zakelijk aan dienen te houden

### 1. Officiële social media kanalen van de organisatie

1. Uitsluitend de hierna genoemde personen vertolken in de media standpunten van de organisatie als geheel:
  - RvB-leden.
  - CvB-leden.
  - Door het Bestuur aangewezen medewerkers.
  - Woordvoerders van de dienst PR Communicatie & Marketing (PRC&M).
2. De social media worden centraal gemonitord door medewerkers van het team Online Communicatie, onderdeel van de dienst PRC&M.
3. Vaak betreft het onderwerpen die betrekking hebben op het Bestuur en het beleid of die anderszins de reputatie van de organisatie raken of beïnvloeden. Het kan daarbij ook specifieke domeinen, MBO Colleges of andere onderdelen van de organisatie betreffen.
4. Andere gebruikers dan die in lid 1 zijn genoemd, zijn niet gerechtigd om namens de organisatie te handelen op social media. Zij verwijzen voor vragen en issues op social media die de organisatie als geheel betreffen voor beantwoording dan wel reactie door naar de daarvoor aangewezen medewerkers of de woordvoerders van de dienst PRC&M.
5. Gebruikers houden zich aan de door PRC&M vastgestelde "richtlijnen voor het gebruik van social media" zoals te vinden op Portaal voor Talent.
6. Gebruikers maken gebruik van het officiële logo en huisstijl van de organisatie zoals vastgesteld door de dienst PRC&M.

### 2. Persoonlijke social media kanalen

1. De organisatie voert geen regie op informatie die gebruikers op persoonlijke titel zenden via social media maar verwacht van gebruikers integriteit bij het gebruik van social media.
2. De organisatie verwacht van gebruikers dan ook dat zij duidelijk aangeven dat ze op persoonlijke titel acteren.
3. Gebruikers die zich via het netwerk of computer van de organisatie bezig houden met social media, dienen de volgende regels in acht te nemen.
  - Maak duidelijk onderscheid tussen zakelijk en privé gebruik van social media.
  - Wees terughoudend met het verstrekken van persoonlijke informatie zoals BSN nummer, adres, telefoonnummer.
  - Ook online is gebruiker gebonden aan de geheimhoudingsplicht met betrekking tot dossiers waar hij mee te maken heeft gekregen of krijgt in het kader van zijn functie. Verwijzingen naar studenten of zakelijke relaties van de organisatie is dan ook niet toegestaan.
4. De organisatie stelt het op prijs indien gebruikers geen onthullende, schokkende of seksueel getinte foto's van zich zelf plaats op social media kanalen. Jurisprudentie heeft uitgewezen dat bij medewerkers met een voorbeeldfunctie zoals het Bestuur maar ook docenten, privacy niet volledig mogelijk is.

**3. Maken en/of publiceren van beeld of geluidsopnames**

1. Gebruikers mogen geen foto's, beeld- of geluidsopnames maken in de school en/of op het schoolterrein tenzij daar voor onderwijsdoeleinden opdracht toe gegeven wordt door een docent of personeelslid van de organisatie of tenzij dit werk gerelateerd is en de persoon die gefotografeerd, opgenomen of gefilmd wordt daarvoor duidelijk toestemming heeft gegeven.
2. Voor elke publicatie van beeld- en of geluidsopnames in de school en/of op het schoolterrein gemaakt is voorafgaande schriftelijke toestemming vereist van alle betrokkenen. De toestemming voor het maken van beeld- of geluidsopnames impliceert geen toestemming voor publicatie.
3. Gebruikers wordt verzocht om door hen gesignaleerde berichten en/of filmpjes (ook van studenten) die zijn gerelateerd aan De organisatie en die niet via de officiële kanalen zijn gepubliceerd, door te sturen naar de dienst PRC&M.
4. Het publiceren van vertrouwelijke informatie over een ander of de organisatie op o.a. social media is niet toegestaan.

## 5. Schending Gedragscode ICT

### 1. Naleving Gedragscode ICT

1. Iedere gebruiker is verplicht zich aan de Gedragscode ICT te houden.
2. Van gebruikers wordt verwacht dat zij bij schending van de ICT gedragscode zoals oneigenlijk gebruik van de computer, fraude, diefstal, intimidatie, discriminatie enz. dit bij een docent, leidinggevende, personeels-adviseur, vertrouwenspersoon of interne klachtencommissie voor medewerkers melden.
3. Bij interpretatieverschillen van de Gedragscode ICT is primair een rol weggelegd voor de leidinggevende/opleidingsmanager.

### 2. Inhoudelijke controle gebruik ICT faciliteiten

1. Het monitoren en controleren van het internet en emailgebruik kan meebrengen dat persoonsgegevens in de zin van de WBP worden verwerkt door de organisatie. Dit wordt inhoudelijk geregeld in het privacyreglement.
2. De organisatie streeft naar een goede balans tussen het bereiken van een verantwoord gebruik van de IT faciliteiten en de bescherming van de privacy van Gebruikers.
3. Monitoring en inhoudelijke controle van het gebruik van ICT-faciliteiten kan uitsluitend plaatsvinden voor onderstaande doeleinden:
  - Systeem en netwerkbeveiliging
  - Voorkomen van uitlekken van vertrouwelijke informatie
  - Tegengaan van (cyber)pesten, discriminatie of seksuele intimidatie
  - Behandelen van geschillen
  - Op vordering van bevoegde instanties
  - Bij vermoeden van ernstige schending van de ICT Gedragscode.
4. Uitsluitend indien concrete verdenkingen bestaan dat een gebruiker deze gedragscode overtreedt kan gedurende een van te voren vastgestelde (korte) periode gerichte controle plaats vinden. De controle beperkt zich in beginsel tot de verkeersgegevens van het internet en email gebruik.
5. De organisatie zal terughoudendheid betrachten bij het inhoudelijke controleren van internet en emailgebruik dat herleidbaar is tot een persoon. Hiertoe wordt uitsluitend bij zwaarwegende redenen toe overgegaan. De controle zal uitsluitend door de Dienst ICT worden uitgevoerd.
6. Bij constatering van ongeoorloofd gebruik van ICT faciliteiten wordt dit zo spoedig mogelijk met de betrokken gebruiker besproken.
7. De organisatie zal emailverkeer van OR leden, CSR leden, Vertrouwenspersoon en Ombudsman niet controleren.

### 3. Procedure

1. Een ieder die meent dat een gebruiker de in de ICT gedragscode opgestelde richtlijnen ernstig overtreedt, kan dit melden aan de directeur van zijn Dienst/MBO College.
2. De directeur van Dienst/MBO College zal bij vermoedens van ernstige schending van de ICT gedragscode door een medewerker eerst overleg voeren met de directeur HRM. De directeur HRM is bevoegd om het besluit te nemen om over te gaan op inhoudelijke controle. De directeur HRM zal dit verzoek neerleggen bij de Dienst ICT.
4. De Dienst ICT informeert de gebruiker dat zijn bestanden inhoudelijk zullen worden gecontroleerd over een alsdan vastgestelde periode. Van de gebruiker wordt verwacht dat deze medewerking verleent op het moment dat een inhoudelijke controle plaatsvindt.
5. Wanneer misbruik van ICT-faciliteiten schade veroorzaakt, zal de organisatie deze schade verhalen op de gebruiker die deze schade veroorzaakt heeft.

### 4. Disciplinaire maatregelen

1. Ernstige overtreding van de ICT Gedragscode kan leiden tot disciplinaire consequenties voor medewerkers of deelnemers. Bij medewerkers kan dit variëren van een berisping tot ontslag op staande voet. Bij studenten kan dit variëren van berisping tot verwijdering van school
2. Van strafbare feiten wordt door de organisatie altijd aangifte gedaan bij de politie.

## **6. Slotbepalingen**

### **1. Vaststellingstraject**

1. Dit reglement is op 30 juni 2014 vastgesteld in de vergadering van het Bestuur.
2. Dit reglement is ter informatie aangeboden aan OR ROCvA, OR ROCvF en GMR VOvA.
3. Dit reglement is ter informatie aangeboden aan de CSR ROCvA en CSR ROCvF.

### **2. Inwerkingtreding en duur reglement**

1. Dit reglement treedt in werking op 1 augustus 2014 voor de duur van 2 jaar.
2. Dit reglement vervangt alle eerdere ICT-reglementen over het gebruik van ICT Faciliteiten.
3. Het reglement kan tussentijds worden gewijzigd op verzoek van het Bestuur of de Dienst ICT.
4. Na 1 schooljaar vindt evaluatie plaats en wordt onderzocht of het reglement naar tevredenheid van alle betrokkenen werkt.
5. Indien partijen geen verzoek tot wijziging van het reglement aan de ander kenbaar hebben gemaakt, wordt het reglement van rechtswege verlengd voor de duur van twee jaar.

# Bijlage 1

## Begrippenlijst

---

## **Bijlage 1. Begrippenlijst**

In de ICT Gedragscode wordt onder de navolgende begrippen het onderstaande verstaan.

<b>Account (netwerkaccount)</b>	De gebruikersnaam en het wachtwoord waarmee een Gebruiker toegang tot een netwerk of een computer kan krijgen. Naast de gebruikersnaam en het wachtwoord bevat een account andere informatie over de Gebruiker, zoals de netwerkschijven, folders en bestanden waarvan de Gebruiker gebruik kan maken.
<b>Cloud</b>	Onder cloud computing verstaan we het leveren of gebruiken van schaalbare diensten (clouddiensten) via internet. Denk bijvoorbeeld backup-voorzieningen, opslagruimte en allerlei applicaties (ERP, CRM, E-mail, tekstverwerking, documentbeheer, agendabeheer, enz.).
<b>Digipass</b>	Een digipass wordt gebruikt voor tweefactoren-authenticatie, waarbij "iets wat je weet" (kennis) en "iets wat je bezit" (digipass) worden gecombineerd om tot een hoger niveau van beveiliging te komen. Het meest wordt dit toegepast om toepassingen voor internetbankieren, applicaties en computers te beveiligen.
<b>Gedraging</b>	Niet alleen het gebruik van communicatiemiddelen en ICT faciliteiten valt hier onder, maar ook het omgaan met smartphones, social media, huisstijlgebruik en spreken over elkaar.
<b>ICT Faciliteiten</b>	Hieronder valt minimaal het gebruik van computer, laptop, smartphones en netwerk in de ruimste zin des woords.
<b>Laptop</b>	Een laptop is een draagbare computer.
<b>Lync</b>	Lync is een oplossing van Microsoft waarin verschillende vormen van communicatie samen zijn gebracht. gebruikers van Lync kunnen overal en altijd gemakkelijk en efficiënt met elkaar communiceren en samenwerken. Lync biedt gebruikers de volgende functies: instant messaging, bellen, videobellen, documenten delen, aanwezigheidsindicator, virtuele vergaderingen.
<b>Netwerk</b>	Een computernetwerk is een systeem voor communicatie tussen twee of meer computers. De communicatie verloopt via netwerkkabels of via een draadloos netwerk.
<b>Sharepoint</b>	SharePoint is een internettoepassing (platformen) van Microsoft voor het opzetten van websites voor informatie-uitwisseling en online samenwerking binnen een organisatie of een groep mensen. Dit is een samenwerkingsverband van ROCvA, ROCvF en VOvA.

<b>Smartphone</b>	Een smartphone is een combinatie van een mobiele telefoon en een persoonlijke digitale agenda. Een smartphone stelt gebruikers in staat om overal en altijd te bellen, foto's te maken, video opnames te maken en om gebruik te maken van allerlei datadiensten (internet, mail, instant messaging, agenda, enz.).
<b>Smartwatch</b>	Een smartwatch is een digitale horloge die door middel van een draadloze verbinding kan communiceren met een smartphone. Een Gebruiker wordt hierdoor in staat gesteld om met een smartwatch te bellen, foto's te maken, video opnames te maken en om gebruik te maken van allerlei datadiensten (internet, mail, instant messaging, agenda, enz.).
<b>Social Media</b>	Social media is een verzamelbegrip voor internet-toepassingen (platformen) waar de gebruikers informatie met elkaar delen op een gebruiksvriendelijke manier. Het gaat dan niet alleen om tekstuele informatie, maar ook geluid (opnamen, muziek) en beeldmateriaal (plaatjes, foto's, video's) worden gedeeld via Social Media.
<b>Tablet</b>	Een tablet is een draagbare computer met een aanraakgevoelig scherm. Dit aanraakscherm wordt gebruikt als invoerapparaat voor de tablet. Een tablet kan worden gebruikt voor video, foto's, tekstverwerking, spellen, internet en tientallen andere toepassingen.
<b>Wi-Fi</b>	Wi-Fi is een certificatielabel voor producten voor draadloze datanetwerken, die werken volgens de internationale standaard IEEE 802.11 (draadloos ethernet of Wi-Fi).