

# ICT-gedragscode en Gedragscode sociale media Medewerkers

# Inhoud

<b>ICT-gedragcode</b> .....	3
Inleiding .....	3
Artikel 1 Algemene normen .....	5
Artikel 2 Computergebruik .....	5
Artikel 3 Werkplek .....	6
Artikel 4 Gebruik je eigen devices (BYOD).....	6
Artikel 5 Software en digitaal lesmateriaal.....	7
Artikel 6 Gebruik van e-mail.....	7
Artikel 7 Gebruik van internet .....	8
Artikel 8 Veilig online .....	8
Artikel 9 Sociale media .....	8
Artikel 10 Gebruik beeld- en geluidsmateriaal.....	9
Artikel 11 Wachtwoorden en pincodes .....	9
Artikel 12 Intellectueel eigendom en vertrouwelijke informatie.....	10
Artikel 13 Meldplicht Datalekken.....	10
Controle gebruik bedrijfsmiddelen .....	10
Artikel 14 Voorwaarden voor controle .....	10
Artikel 15 Uitvoering van de controle .....	11
Artikel 16 Disciplinaire maatregelen .....	11
Artikel 17 Bezwaar en beroep.....	12
Artikel 18 Slotbepaling .....	12
<b>Gedragcode sociale media</b> .....	13
Inleiding .....	13
Artikel 1 Uitgangspunten.....	13
Artikel 2 Doelgroep en reikwijdte .....	13
Artikel 3 Regels voor medewerkers .....	13
Artikel 4 Regels voor medewerkers tijdens privésituaties .....	14
Artikel 5 Sancties en gevolgen voor medewerkers.....	14
Artikel 6 Slotbepaling .....	15

# ICT-gedragcode

## Inleiding

Het gebruik van internet, computernetwerk, (kern-)systemen en e-mail is voor alle medewerkers van Onderwijsgroep Tilburg noodzakelijk om de werkzaamheden te kunnen verrichten. Bij deze werkzaamheden wordt gebruik gemaakt van veel informatie en gegevens, waaronder persoonsgegevens. De (ICT-)faciliteiten en de verschillende systemen en gegevens worden in deze ICT-gedragcode bedrijfsmiddelen genoemd. Onder bedrijfsmiddelen worden in ieder geval verstaan:

- Hardware: computer, laptop, tablet, telefoon, hardware token.
- Software (of -systemen): alle applicaties voor het uitvoeren van de werkzaamheden, zoals de school e-mailomgeving, Microsoft Office, (administratie)systemen (zoals EduArte, Magister en Afas) en (online) digitaal lesmateriaal, maar ook apps op (mobiele) devices.
- Informatie en (persoons)gegevens: rapportages, student- en leerlingdossiers, gegevens in e-mails. Hierbij vraagt de verwerking van persoonsgegevens vanuit de privacywetgeving extra maatregelen en aandacht.
- Internetgebruik: het bezoeken van het World Wide Web, het gebruik van e-mail en diensten en maar ook sociale media.

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers van Onderwijsgroep Tilburg wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen (devices) inzetten om hun werkzaamheden uit te voeren.

De afspraken in deze gedragcode gelden voor alle locaties van waaruit werkzaamheden worden verricht en voor alle devices waarmee het werk wordt uitgevoerd. De gedragcode geldt voor iedereen die werkzaam is bij Onderwijsgroep Tilburg, ook voor uitzendkrachten, tijdelijke werknemers (gedetacheerden) en stagiaires. De gedragcode geldt voor alle externen die, via een account van Onderwijsgroep Tilburg, toegang hebben tot de bedrijfsmiddelen van de organisatie.

## Uitgangspunten ICT-gedragcode

Deze ICT-gedragcode bevat regels voor het gebruik van de bedrijfsmiddelen door medewerkers en over de controle op de naleving hiervan.

Het doel van deze gedragcode is om de normen en uitgangspunten vast te leggen ten aanzien van:

- de systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik.
- het tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten.
- de bescherming van privacy gevoelige informatie waaronder persoonsgegevens van de medewerkers, studenten, leerlingen en ouders en daarmee het beschermen van de privacy en veiligheid van alle betrokkenen.
- de bescherming van vertrouwelijke informatie van Onderwijsgroep Tilburg en van medewerkers, studenten, leerlingen en ouders.
- het voorkomen en tegengaan van misbruik van bedrijfsmiddelen.
- de bescherming van de intellectuele eigendomsrechten van Onderwijsgroep Tilburg en derden.
- het voorkomen van negatieve publiciteit.
- de kosten- en capaciteitsbeheersing.

De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. Onderwijsgroep Tilburg zal dan ook de controle en handhaving van deze regels conform de arbeids- en privacywetgeving uitvoeren. Hierbij is het uitgangspunt een goede balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers op de werkplek. Gegevens worden alleen verzameld en gebruikt voor deze doelen. In het bijzonder zal het College van Bestuur de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang. Medewerkers met geautoriseerde toegang zijn op basis van de vigerende CAO verplicht tot geheimhouding.

Onderwijsgroep Tilburg streeft in het kader van handhaving van dit document naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele medewerkers zo veel mogelijk beperken. Het College van Bestuur zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in het gedrag van individuele personen.

### **Eigen verantwoordelijkheid en privégebruik**

Het gebruik van door Onderwijsgroep Tilburg verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle devices die zakelijk worden gebruikt (inclusief eigen devices) worden niet uitgeleend of aan anderen ter beschikking gesteld zonder aanvullende (beveiligings)maatregelen. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen.

### **Verschillende soorten gegevens**

Het College van Bestuur is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van data en (persoons) gegevens.

Onderwijsgroep Tilburg onderscheidt drie typen gegevens:

- Openbare gegevens: dit zijn gegevens die juist voor publicatie bedoeld zijn.
- Interne gegevens: dit zijn gegevens die alleen voor gebruik en verwerking binnen de organisatie bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- Vertrouwelijke gegevens: dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen de organisatie toegankelijk zijn. Denk hierbij aan (bijzondere) persoonsgegevens, personeels- en salarisgegevens of aanbestedingsgegevens.

Persoonsgegevens verdienen bijzondere aandacht. Dit zijn gegevens die een persoon betreffen én waardoor een persoon geïdentificeerd of identificeerbaar is. Denk hierbij aan naamgegevens, e-mailadressen, maar ook telefoonnummers van zowel medewerkers, als studenten, leerlingen en ouders.

De privacywetgeving verplicht elk individu om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat Onderwijsgroep Tilburg schriftelijk afspraken maakt met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt. Denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk of digitale examens.

Onderwijsgroep Tilburg heeft een Functionaris Gegevensbescherming. Deze communiceert intern de gedragsregels die horen bij het verwerken van persoonsgegevens. Persoonsgegevens moeten altijd met uiterste zorgvuldigheid verwerkt en gedeeld worden.

Als persoonsgegevens toegankelijk en of inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot deze gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en ook voor Onderwijsgroep Tilburg.

Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt Onderwijsgroep Tilburg afspraken over:

- de verwerking en verspreiding van vertrouwelijke- en persoonsgegevens. Er worden niet meer gegevens verwerkt dan noodzakelijk om het doel te bereiken.
- de uitwisseling van gegevens, waarbij aan de ontvanger wordt aangegeven wat de ontvanger wel of niet mag doen met de gegevens.
- de opslag en verspreiding van gegevens, waarbij alléén gebruik gemaakt wordt van door Onderwijsgroep Tilburg goedgekeurde bedrijfsmiddelen.

Van medewerkers van Onderwijsgroep Tilburg en/of externen, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bijvoorbeeld personeelsdossiers, vertrouwelijke enquêtegegevens, student- of leerlingdossiers wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. Zij worden geacht de privacywetgeving na te leven en op geen enkele wijze informatie, waarvan redelijkerwijze kan worden aangenomen dat deze vertrouwelijk of privacygevoelig is, zonder toestemming van betrokkene of leidinggevende te gebruiken en/of naar buiten te brengen.

In deze ICT-gedragscode zijn de regels met betrekking tot het verantwoord gebruik van de bedrijfsmiddelen van Onderwijsgroep Tilburg door medewerkers vastgelegd en wat dit voor de medewerkers in de dagelijkse praktijk betekent.

## **Artikel 1 Algemene normen**

Iedere medewerker voldoet in ieder geval aan de volgende algemene gedragsnormen:

- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen (door middel van beveiligingsmaatregelen).
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild.
- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering door het sturen van een e-mail aan servicedesk@onderwijsgroep Tilburg.nl of een telefonische melding bij de ICT-helppdesk (Zie hiervoor ook de procedure meldplicht datalekken van Onderwijsgroep Tilburg).
- Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht.
- Voorkom het lekken van interne en vertrouwelijke informatie.

## **Artikel 2 Computergebruik**

Voor het uitoefenen van de werkzaamheden stelt Onderwijsgroep Tilburg aan de medewerker computer- en netwerkfaciliteiten (bedrijfsmiddelen) ter beschikking. Het gebruik van deze bedrijfsmiddelen is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Sla (persoons)gegevens alleen op in de daarvoor aangewezen systemen.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Sluit na gebruik de computer af of log uit.
- Meld storingen van beheerde werkplekken bij de ICT-helppdesk via de SelfServiceDesk.
- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.
- Weet welke gegevens er mogen worden gebruikt en welke ICT-voorzieningen kunnen worden ingezet bij het verrichten van de verschillende werkzaamheden.

- Versleutel alle gegevens met betrekking tot Onderwijsgroep Tilburg, indien deze gegevens, om welke reden dan ook, elders opgeslagen worden.

### **Artikel 3    Werkplek**

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen waartoe zij geen rechten hebben en/of laat gegevens niet (onbedoeld) lekken. Als aanvullende regels op computergebruik gelden voor de werkplek de volgende clean desk en clear screen regels:

- Vergrendel bij het tijdelijk verlaten van de werkplek de computer (Windowstoets + L).
- Verwijder interne en vertrouwelijke documenten bij het voor langere tijd verlaten van de werkplek.
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via een beamer) mee kan kijken. Sluit het e-mail programma af en zorg voor een opgeruimd digitaal bureaublad.
- Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan.
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar.

Let op: Als persoonsgegevens toegankelijk en inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot die gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Weet dat beveiligingsincidenten en mogelijke datalekken gemeld moeten worden volgens de procedure meldplicht datalekken van Onderwijsgroep Tilburg.

### **Artikel 4    Gebruik je eigen devices (BYOD)**

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor Onderwijsgroep Tilburg worden uitgevoerd. Onderwijsgroep Tilburg is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de organisatie.

Voor 'own devices' ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen voor de eigen devices worden genomen:

- Beveilig het device met een verificatie methode die door de leverancier wordt aanbevolen zoals met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode of veegpatroon.
- Vergrendel het device bij het verlaten van de werkplek (Windowstoets + L of lockscreen).
- Sla persoonsgegevens van Onderwijsgroep Tilburg niet op het eigen device op; dit is niet toegestaan.
- Sla persoonsgegevens van Onderwijsgroep Tilburg niet op buiten de applicaties die hiervoor binnen de organisatie bedoeld zijn, zoals de systemen en apps van EduArte, Magister, AFAS Pocket en de OneDrive.
- Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot Onderwijsgroep Tilburg als deze, om welke reden dan ook, niet op het netwerk opgeslagen worden (denk hierbij aan het eigen device of usb-stick).
- Scheid (versleutelde) gegevens van Onderwijsgroep Tilburg en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen device.
- Houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks).
- Neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het periodiek (minimaal maandelijks) scannen van het device.

Onderwijsgroep Tilburg mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van Onderwijsgroep Tilburg moet de medewerker zelf aantonen dat de bovenstaande maatregelen worden toegepast.

## **Artikel 5 Software en digitaal lesmateriaal**

Het gebruik van digitaal lesmateriaal is niet meer weg te denken. Dit lesmateriaal staat steeds meer online waarbij steeds vaker persoonsgegevens worden uitgewisseld. De privacywetgeving eist dat elke organisatie vooraf aan het gebruik van dergelijk materiaal bekijkt wat de invloed ervan is op de privacy, dit kan specifieke maatregelen tot gevolg hebben.

De onderstaande regels gelden voor installatie en gebruik van software en (online)digitaal lesmateriaal:

- Installeren van software wordt bij Onderwijsgroep Tilburg alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen.
- Bij het gebruik van online software, app's en digitaal lesmateriaal, wordt gekeken of er persoonsgegevens bij verwerkt worden.
- Een verwerkersovereenkomst wordt afgesloten met elke leverancier van (online)software, die in opdracht van Onderwijsgroep Tilburg persoonsgegevens verwerkt. Ook als de (online)software gratis is. Regel de verwerkersovereenkomst vooraf aan het gebruik.
- Aanvragen van digitaal lesmateriaal en/of andere software volgt bij Onderwijsgroep Tilburg de afgesproken aanvraagprocedure door middel van een wijzigingsverzoek. Hiervoor is een aanvraagformulier (wijzigingsverzoek) beschikbaar wat als uitgangspunt dient voor eventuele wettelijk verplichte aanvullende privacy- en/of beveiligingsmaatregelen.

## **Artikel 6 Gebruik van e-mail**

Onderwijsgroep Tilburg stelt een e-mailsysteem en een bijbehorende mailbox aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik van e-mailfaciliteiten is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Gebruik het school e-mailadres alléén voor werk gerelateerde zaken.
- Gebruik voor privé e-mail en privé gerelateerde zaken een eigen privé e-mailadres.
- Ontvangen van privé e-mail op het zakelijke e-mailadres is beperkt toegestaan. Uit de onderwerp-regel van de privé e-mail dient te blijken dat het om privé zaken gaat. Privé e-mails op het zakelijke e-mailadres dienen in een privé map in de zakelijke mailomgeving te worden opgeslagen.
- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.
- Het is niet toegestaan e-mail te gebruiken voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of voor berichten die kunnen aanzetten tot haat en geweld.
- Koppelt en synchroniseert een medewerker de zakelijke school e-mail met een eigen device (tablet, telefoon) dan kan Onderwijsgroep Tilburg, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het privé device gewist worden.

## Artikel 7 Gebruik van internet

Onderwijsgroep Tilburg stelt het gebruik van internet en de bijbehorende faciliteiten aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik hiervan is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Beperkt persoonlijk gebruik is toegestaan, mits dit
  - niet storend is voor de dagelijkse werkzaamheden
  - niet voor commerciële doeleinden is, en
  - geen verboden gebruik oplevert.
- Het is niet toegestaan om
  - op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten
  - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron
  - onder leestijd internettoegang te gebruiken voor privédoeleinden
  - deel te nemen aan kansspelen.
- Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale netwerken en andere vergelijkbare communicatienetwerken over alle aan de organisatie verbonden betrokkenen en activiteiten. Dit geldt in het bijzonder ook voor internetgebruik buiten het netwerk met betrekking tot aan de organisatie verbonden betrokkenen en activiteiten.

## Artikel 8 Veilig online

We brengen met z'n allen steeds meer tijd online door. Hierbij worden steeds meer mobiele devices gebruikt. Menselijk (online)handelen staat veelal aan de basis van een datalek.

Onderwijsgroep Tilburg verwacht van medewerkers dat zij:

- het onderscheid kennen tussen betrouwbare en onbetrouwbare websites.
- bij het verwerken van persoonsgegevens alléén gebruik maken van bekende én beveiligde draadloze netwerken.
- weten wat malware is, het kunnen herkennen en weten hoe te handelen.
- terughoudend zijn met het online achterlaten van gegevens met betrekking tot Onderwijsgroep Tilburg
- controleren of er daadwerkelijk van een bekend én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes. (Een netwerk kan bekend zijn omdat het een Onderwijsgroep Tilburg netwerk is, Eduroam of het eigen draadloze netwerk thuis is).

## Artikel 9 Sociale media

Sociale media vormen een verzamelbegrip voor online platforms waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. (Externe) Sociale media is bedoeld voor het onderhouden van netwerken ten behoeve van professionalisering (zoals collega's van andere onderwijsinstellingen volgen op Twitter, ervaringen uitwisselingen via LinkedIn of deelnemen aan vakgroepen op Facebook), het publiceren van wervingsmateriaal, het aankondigen van openbaar nieuws en het promoten van een opleiding of school. Het gaat hierbij niet alleen om informatie in de vorm van tekst (nieuws, artikelen). Ook geluid (podcasts, muziek) en beeld (fotografie, video) worden gedeeld via sociale media. De essentie van sociale media is dat iemand er informatie deelt over zichzelf, over anderen of over een bepaald onderwerp.



Voor gebruik van sociale media geldt als uitgangspunt dat het digitale gedrag op sociale media niet afwijkt van de reguliere fatsoens- en gedragsnormen binnen de organisatie. Medewerkers zijn altijd de vertegenwoordiger van Onderwijsgroep Tilburg ook als zij online een privémening verkondigen.

Bij Onderwijsgroep Tilburg gelden de volgende afspraken voor het gebruik van sociale media:

- Deel op verantwoorde wijze kennis via sociale media rekening houdend met de goede naam van Onderwijsgroep Tilburg en iedereen die hierbij betrokken is.
- Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens Onderwijsgroep Tilburg gedaan wordt.
- Publiceer geen vertrouwelijke informatie op sociale media en let op wat je deelt.
- Publiceer geen beeldmateriaal van studenten en leerlingen.
- Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn. Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren.
- Neem contact op met je leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met Onderwijsgroep Tilburg.
- De communicatie met studenten, leerlingen en ouders loopt enkel via de daarvoor aangewezen formele kanalen (zoals Teams, Magister, EduArte, schoolmail e.d.). Let op als je als medewerker met een privé account 'vrienden' wordt met studenten, leerlingen en ouders op sociale media, dan wel als je via privéberichten met hen communiceert.
- Inzetten van externe sociale media waar Onderwijsgroep Tilburg geen (verwerkers-) overeenkomst en licenties mee heeft, is in het lesprogramma, de begeleiding van de student of de leerling, en het contact met studenten, leerlingen en ouders niet toegestaan. Hiervoor worden eigen interne (communicatie)middelen en (les)materialen ingezet.
- Aanvullende afspraken rondom sociale media in het algemeen heeft Onderwijsgroep Tilburg vastgelegd in een afzonderlijke gedragscode sociale media voor medewerkers.

## **Artikel 10 Gebruik beeld- en geluidsmateriaal**

Het gebruiken van beeld- en geluidsmateriaal, het delen van foto's, video's en geluidsfragmenten van studenten en leerlingen door medewerkers vallend onder Onderwijsgroep Tilburg mag alleen als daar vooraf toestemming voor gegeven is door ouders als de student of leerling jonger is dan 16 jaar of de student of leerling zelf als deze ouder dan 16 jaar is. Zonder deze toestemming mogen geen foto's, video's en geluidsfragmenten van studenten en leerlingen gebruikt worden.

- Onderwijsgroep Tilburg verwijst hierbij naar de richtlijn die is opgesteld voor het gebruik en toestemming van beeldmateriaal.
- Voor de afspraken rondom het delen van beeld- en geluidsmateriaal via sociale media gelden de richtlijnen die genoemd worden bij het gebruik van sociale media.

## **Artikel 11 Wachtwoorden en pincodes**

Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en devices (computer, laptop, telefoon) begint met een goed wachtwoord. Een lang wachtwoord of een 'wachtzin' is beter dan een kort, complex wachtwoord. Voor het gebruik van wachtwoorden gelden onderstaande afspraken:

- Wachtwoorden moeten minimaal 8 tekens bevatten, met minstens drie van de volgende vier elementen: kleine letter, hoofdletter, cijfer of speciaal teken (!@#\$%^&\*())
- Wachtwoorden moeten volgens de afspraken binnen Onderwijsgroep Tilburg op aangegeven tijden vervangen worden.
- Beveilig de toegang tot devices met een pincode of veegpatroon.
- Gebruik niet voor elk systeem hetzelfde wachtwoord, indien geen 2FA wordt gebruikt.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.

## **Artikel 12 Intellectueel eigendom en vertrouwelijke informatie**

De medewerker dient vertrouwelijke en/of privacygevoelige informatie, waaronder persoonsgegevens waar hij in het kader van het werk toegang tot heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.

De medewerker maakt geen inbreuk op de intellectuele eigendomsrechten van Onderwijsgroep Tilburg en derden en respecteert licentieafspraken die van toepassing zijn binnen de organisatie. De zeggenschap over de informatie van Onderwijsgroep Tilburg berust bij de organisatie. De medewerker heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de organisatie.

De medewerker besteedt bijzondere aandacht aan het treffen van maatregelen zoals in deze gedragscode genoemd, indien in het kader van het uitvoeren van de werkzaamheden de verwerking van vertrouwelijke informatie buiten Onderwijsgroep Tilburg noodzakelijk is, zoals via e-mail, in niet instellingsgebonden cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur (USB-apparaten, tablets, etc.). Onder maatregelen valt in ieder geval de verplichting voor de medewerker om gebruik te maken van versleutelde externe opslagmedia of versleutelde eigen client-apparatuur.

Indien Onderwijsgroep Tilburg met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten nadere voorschriften heeft opgesteld, dient de medewerker deze strikt op te volgen.

## **Artikel 13 Meldplicht Datalekken**

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken direct melden volgens de procedure meldplicht datalekken van Onderwijsgroep Tilburg.

## **Controle gebruik bedrijfsmiddelen**

Onderwijsgroep Tilburg handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving. Onderwijsgroep Tilburg zal bij controle rondom het gebruik van bedrijfsmiddelen op basis van deze gedragscode uitgaan van de juiste balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers.

## **Artikel 14 Voorwaarden voor controle**

- Controle van persoonsgegevens met betrekking tot gebruik van bedrijfsmiddelen vindt slechts plaats in het kader van handhaving van de doelen van deze gedragscode.
- Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
- Uitsluitend bij een ernstig vermoeden van schending van deze gedragscode door een medewerker of een groep medewerkers, kan gedurende een vastgestelde (korte) periode, in opdracht van het College van Bestuur gerichte controle op individueel gebruik van bedrijfsmiddelen plaatsvinden.
- Gerichte controle en onderzoek vinden uitsluitend plaats na schriftelijke opdracht van het College van Bestuur, na advies van Juridische Zaken, waarbij de reden vermeld zal worden waarom tot dit gerichte onderzoek zal worden overgegaan. Het onderzoek wordt uitgevoerd door één of meer daartoe aangewezen medewerker(s) van de afdeling Operationele Services (ICT Services).
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van het College van Bestuur, controle op de inhoud plaats.
- Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.

- Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken medewerker besproken. Onderwijsgroep Tilburg zal de medewerker op verzoek inzage verschaffen in de gegevens over het eigen gebruik. De medewerker wordt gewezen op de consequenties wanneer niet wordt gestopt met het ongeoorloofd gebruik.
- E-mailberichten van leden van de medezeggenschap, van vertrouwenspersonen, bedrijfsartsen en van een ieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Dit geldt niet voor de (technische) veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden, indien het berichtenverkeer niet veilig gebeurt.

## **Artikel 15    Uitvoering van de controle**

- 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.
- De controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.
- De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens.
- De controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.
- De systeembeheerder(s) zijn aan geheimhouding gebonden als men om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.
- Door Onderwijsgroep Tilburg worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- Door Onderwijsgroep Tilburg worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

## **Artikel 16    Disciplinaire maatregelen**

Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het College van Bestuur van Onderwijsgroep Tilburg, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen. Hieronder vallen onder andere een waarschuwing/schriftelijke berisping, schadevergoeding, melding of aangifte bij de politie, schorsing, overplaatsing en/of beëindiging van de arbeidsovereenkomst. Een ontslag op staande voet behoort tot de mogelijkheden. Aanvullende maatregelen kunnen onder meer bestaan uit het in bewaring nemen van devices en het verwijderen van berichten en/of beelden daarop.

Medewerkers die zich niet aan deze gedragscode houden, worden zo spoedig mogelijk door hun leidinggevende op hun gedrag aangesproken. Zij krijgen daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. Medewerker en leidinggevende maken dan afspraken voor de toekomst en bepalen de mogelijke maatregelen bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in deze gedragscode bepaalde. Ook kan de toegang tot e-mail of internet worden beperkt of geheel worden afgesloten. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens worden getroffen, zoals een constatering van een automatisch filter of blokkade. Er worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

## **Artikel 17 Bezwaar en beroep**

Als de medewerker het niet eens is met de (voorgenomen) disciplinaire maatregel, dan kan daar in een aantal gevallen bezwaar en/of beroep tegen worden ingesteld. Dit is meestal geregeld in de arbeidsovereenkomst, de van toepassing zijnde CAO en het Reglement van de Interne geschillencommissie.

## **Artikel 18 Slotbepaling**

Deze gedragscode treedt in werking per 1 augustus 2021. De Ondernemingsraad en Gemeenschappelijke Medezeggenschapsraad hebben op 27 mei 2021 ingestemd met artikel 14 en 15 van deze gedragscode. Wijzigingen worden alleen ingevoerd nadat de Ondernemingsraad en Gemeenschappelijke Medezeggenschapsraad hiermee hebben ingestemd. In gevallen waarin deze gedragscode niet voorziet, beslist het College van Bestuur. Deze gedragscode komt ter vervanging van de huidige ICT-gedragscode voor medewerkers van Onderwijsgroep Tilburg.

# Gedragcode sociale media

## Inleiding

Sociale media is een verzamelbegrip voor online platforms waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Onder de noemer sociale media worden onder andere weblogs of blogs, WhatsApp, videosites als YouTube en sociale netwerken als Facebook, Twitter, LinkedIn en Instagram geschaard. Via deze media worden verhalen, kennis, ervaringen en beeld- en/of geluidmateriaal gedeeld.

Sociale media biedt de mogelijkheid om te laten zien dat de medewerker trots is op de school en kan een bijdrage leveren aan een positief imago van de school. Medewerkers moeten beseffen dat met berichten op sociale media (onbewust) de goede naam van de school en van collega's, studenten en ook geschaad kunnen worden. Om deze reden dient door medewerkers bewust met sociale media omgegaan te worden. Voor het gebruik van sociale media geldt tegenover alle betrokkenen de reguliere fatsoensnormen. Onderwijsgroep Tilburg vindt het belangrijk dat medewerkers, studenten en leerlingen, ouders en andere betrokkenen verantwoord omgaan met sociale media. Onderwijsgroep Tilburg heeft daarom gedragscodes opgesteld om een ieder die bij Onderwijsgroep Tilburg betrokken is of zich daarbij betrokken voelt daarvoor richtlijnen te geven.

## Artikel 1   Uitgangspunten

1. Onderwijsgroep Tilburg onderkent het belang van sociale media.
2. Deze gedragscode draagt bij aan een goed en veilig school- en onderwijsklimaat.
3. Deze gedragscode bevordert dat medewerkers op verantwoorde wijze communiceren op sociale media en daarbij de reguliere fatsoensnormen in acht nemen. Dit betekent dat we respect voor de school en elkaar hebben, dat we verdraagzaam zijn 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 gedragscode dient ervoor alle betrokkenen bij Onderwijsgroep Tilburg te beschermen tegen de mogelijke negatieve gevolgen van de sociale media.

## Artikel 2   Doelgroep en reikwijdte

1. Deze gedragscode is bedoeld voor medewerkers en personen die op een andere manier aan de school verbonden zijn. De gedragscode geldt voor iedereen die werkzaam is bij Onderwijsgroep Tilburg, ook voor uitzendkrachten, tijdelijke werknemers (gedetacheerden) en stagiaires.
2. De regels in deze gedragscode hebben betrekking op berichten die direct of indirect gerelateerd zijn aan de school en de organisatie of wanneer sprake is van overlap tussen school, werk en privé.

## Artikel 3   Regels voor medewerkers

1. Het is medewerkers toegestaan om kennis en informatie over de school te delen op sociale media, mits het geen persoonsgegevens<sup>1</sup> betreft en de school of andere betrokkenen niet schaadt. Daarbij nemen zij de reguliere fatsoensnormen in acht en houden zij zich aan de wet. Gedragingen en uitlatingen, zoals pesten, kwetsen, stalken, bedreigen, hacken, radicalisering en sexting zijn uit den boze. Deze worden geacht in strijd te zijn met de reguliere fatsoensnormen en/of (mogelijk) een strafbaar karakter te hebben.

---

<sup>1</sup> Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identicator zoals een naam, een identificatienummer, locatiegegevens, een online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4 AVG).

2. Het is medewerkers niet toegestaan om vertrouwelijke informatie op sociale media te delen.
3. Het is medewerkers niet toegestaan om tijdens de lessen actief te zijn op sociale media dan wel beeld- en/of geluidsopnamen te maken en/of te verspreiden, tenzij door de schooldirecteur hiervoor nadrukkelijk vooraf expliciet toestemming is gegeven. Het voorgaande geldt ook bij lessen die op afstand (online) worden gegeven.
4. Medewerkers zijn persoonlijk verantwoordelijk voor de inhoud die zelf wordt gepubliceerd op sociale media en kunnen daarop aangesproken worden. Dat geldt ook voor het doorsturen (forwarden) en herplaatsen (re-tweeten) van berichten.
5. Elke medewerker dient zich ervan bewust te zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na verwijdering van het bericht.
6. De medewerker vraagt aantoonbaar schriftelijke toestemming aan ouders of aan studenten en leerlingen ouder dan 16 jaar om foto-, film- en geluidsopnamen van aan school gerelateerde situaties, waarop zij zijn afgebeeld, op het school-account van sociale media te zetten.
7. Medewerkers zullen met een privéaccount geen 'vrienden' worden van studenten en ouders op sociale media, dan wel via privéberichten op sociale media met hen communiceren. Ook de student en/of ouder dient derhalve het sturen van 'vriendschap' verzoeken en privéberichten naar een privéaccount van een medewerker achterwege te laten. Het contact met Onderwijsgroep Tilburg en haar medewerkers loopt enkel via de daarvoor aangewezen formele kanalen (zoals Teams, EduArte, Magister, zakelijke mailaccount e.d.).
8. Indien een medewerker kennis heeft van ontoelaatbare en/of grensoverschrijdende communicatie in woord, beeld en/of geluid dan dient dat gemeld te worden bij de schooldirecteur, leidinggevende of het College van Bestuur.

#### **Artikel 4 Regels voor medewerkers tijdens privésituaties**

1. Het is de medewerker toegestaan om school- en werk-gerelateerde onderwerpen te publiceren mits het geen persoonsgegevens van de school, haar medewerkers, studenten, leerlingen, ouders en andere betrokkenen betreft. Ook mag de publicatie de naam van de school en Onderwijsgroep Tilburg niet schaden.
2. Het is voor medewerkers niet toegestaan standpunten en/of overtuigingen uit te dragen die in strijd zijn met de missie en visie van Onderwijsgroep Tilburg en de uitgangspunten van deze gedragscode.
3. Indien de medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met de onderwijsinstelling dient hij te vermelden dat hij medewerker is van de school en/of Onderwijsgroep Tilburg.
4. Als de medewerker over Onderwijsgroep Tilburg publiceert dient hij het bericht te voorzien van de mededeling dat de standpunten en meningen in dit bericht de eigen persoonlijke mening zijn (op persoonlijke titel zijn geschreven) en los staan van eventuele officiële standpunten van Onderwijsgroep Tilburg.

#### **Artikel 5 Sancties en gevolgen voor medewerkers**

1. Medewerkers houden zich bij de vervulling van hun functie en het uitvoeren van de werkzaamheden aan de regels die ten behoeve van de goede gang van zaken door Onderwijsgroep Tilburg door middel van instructies en/of reglementen zijn vastgesteld en kenbaar zijn gemaakt, waaronder deze gedragscode.
2. Medewerkers die in strijd handelen met deze gedragscode maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie over dit onderwerp wordt opgenomen in het personeelsdossier.

3. Indien Onderwijsgroep Tilburg de wijze van communiceren door een medewerker als 'grensoverschrijdend' kwalificeert, dan kan hiervan melding bij de vertrouwensinspecteur worden gemaakt.
4. Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het College van Bestuur van Onderwijsgroep Tilburg, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen. Hieronder vallen onder andere een waarschuwing/schriftelijke berisping, schadevergoeding, melding of aangifte bij de politie, schorsing, overplaatsing en/of beëindiging van de arbeidsovereenkomst. Een ontslag op staande voet behoort tot de mogelijkheden. Aanvullende maatregelen kunnen onder meer bestaan uit het in bewaring nemen van devices en het verwijderen van berichten en/of beelden daarop.
5. Wanneer bij uitlatingen of gedragingen van medewerkers mogelijk sprake is van een strafbaar feit, kan door Onderwijsgroep Tilburg melding of aangifte bij de politie worden gedaan.

## **Artikel 6 Slotbepaling**

1. Deze gedragscode treedt in werking op 1 januari 2021, wordt twee jaarlijks geëvalueerd en vastgesteld door het College van Bestuur. De eerstvolgende evaluatie vindt plaats voor 1 januari 2023 of zoveel eerder als nodig is.
2. De Ondernemingsraad en Gemeenschappelijke Medezeggenschapsraad hebben op 27 mei 2021 ingestemd met deze gedragscode.
3. Het College van Bestuur kan deze gedragscode met instemming van de Ondernemingsraad en Gemeenschappelijke Medezeggenschapsraad wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering ervan aan de medewerkers bekend gemaakt