ICT-Protocol

gedragscode verantwoord gebruik bedrijfsmiddelen

Vastgesteld

Versie	Datum	Naam	Functie
1	17 november 2020	A.H. Hoekstra	voorzitter CvB

Instemming GMR d.d.: 8 december 2020

Inhoudsopgave

1. Inleiding

Het gebruik van internet, computernetwerk en e-mail is voor alle medewerkers van de school noodzakelijk om de werkzaamheden te kunnen verrichten. Bij deze werkzaamheden wordt gebruik gemaakt van veel gegevens, waaronder persoonsgegevens.

Aan het gebruik van deze middelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers van het Regius College wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor de school uit te voeren.
De afspraken in dit document gelden voor alle locaties van waaruit (school)werkzaamheden worden verricht en voor alle devices waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij het Regius College, ook voor stagiaires, LIO, uitzendkrachten en tijdelijke werknemers.

De (ict)faciliteiten en de verschillende gegevens worden in dit document bedrijfsmiddelen genoemd. Onder bedrijfsmiddelen worden in ieder geval verstaan:

- Hardware: pc, laptop, Chromebook, tablet, telefoon, hardware token (tag).
- Software (of -systemen): alle applicaties voor het uitvoeren van de werkzaamheden, zoals de school e-mailomgeving, Google omgeving en Clouddiensten, administratiesystemen en (online)digitaal lesmateriaal maar ook apps op (mobiele) devices.
- Informatie en (persoons)gegevens: rapportages, leerling dossiers, gegevens in e-mails. Hierbij vraagt de verwerking van persoonsgegevens vanuit de privacywetgeving extra maatregelen.
- Internetgebruik: het bezoeken websites, het gebruik van e-mail en andere onlinediensten maar ook sociale media zoals Facebook, LinkedIn, Instagram en Twitter.

1.1 Uitgangspunten ICT-protocol

Dit protocol legt regels vast voor het gebruik van de bedrijfsmiddelen door medewerkers en over de controle op de naleving hiervan. Het doel van dit protocol is om de normen en uitgangspunten vast te leggen ten aanzien van:

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

1.2 Eigen verantwoordelijkheid

Het gebruik van door het Regius College verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle devices die voor schoolwerk worden gebruikt worden niet uitgeleend of aan anderen ter beschikking gesteld zonder aanvullende (beveiligings)maatregelen zoals tweeweg authenticatie en het aanmaken van persoonlijke accounts.

1.3 Verschillende soorten gegevens

Het Regius College is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens. We onderscheiden 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 het Regius College bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- **Vertrouwelijke gegevens**; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen het Regius College toegankelijk zijn. Denk hierbij aan (bijzondere) persoonsgegevens, personeelsgegevens of aanbestedingsgegevens.

De privacywetgeving verplicht elk individu om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat het Regius College schriftelijk afspraken maakt in verwerkersovereenkomsten met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk).

Het Regius College heeft een Functionaris voor gegevensbescherming aangesteld. Deze houdt toezicht op de toepassing en naleving van de AVG binnen onze school.

Als persoonsgegevens toegankelijk en of inzichtelijk zijn voor personen, die geen toegang behoren 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 het Regius College.

Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt het Regius College 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;
- opslag en verspreiding van gegevens, waarbij alléén gebruik gemaakt wordt van door het Regius College goedgekeurde bedrijfsmiddelen. Dus bijvoorbeeld geen opslag op de harde schijf van een privé device of USB stick.

Van medewerkers van het Regius College en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bv. personeelsdossiers, vertrouwelijke enquêtegegevens, zorgdossiers etc. wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. Dat zij de privacywetgeving hanteren 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.

2. ICT-protocol

In dit ICT-protocol geeft het Regius College aan wat de afspraken zijn met betrekking tot verschillende onderwerpen rondom het gebruik van bedrijfsmiddelen en wat dit voor de medewerkers in de dagelijkse praktijk betekent.

2.1 Algemene normen

Iedere medewerker voldoet aan de volgende algemene normen voor ‘zorgvuldigheid’ (niet uitputtend):

- Ga zorgvuldig om met persoonsgegevens.
- Voorkom het lekken van interne en vertrouwelijke informatie.
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen (beveiligingsmaatregelen).
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild (bijvoorbeeld door jailbreaks[1]).
- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering bij de afdeling ICT (zie ook de procedure meldplicht datalekken van het Regius College).

2.2 Computer- en netwerkgebruik

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

- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.
- Weet welke gegevens er mogen worden gebruikt (mag iedereen het zien?) en welke ICT-voorzieningen kunnen worden ingezet (is het veilig genoeg?) bij het verrichten van de verschillende schoolwerkzaamheden.
- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op (opslag in bijvoorbeeld een persoonlijke dropbox, of op een USB-stick is niet toegestaan).
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Gebruik van tweeweg authenticatie is verplicht voor onze cloudproducten (zoals SOM-today, Google omgeving en Afas).
- Sluit na gebruik de computer af of log uit.
- Het aansluiten van eigen apparatuur (zoals laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (draadloze) netwerkaansluitingen. De af-

[1] *Jailbreak (letterlijk: (gevangenis)uitbraak) is een Engelse term voor de handeling die het mogelijk maakt om op een iPhone, iPod touch, iPad en Apple TV softwaretoepassingen te laden die door de firma Apple niet erkend zijn.*

deling ICT kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit protocol, zoals het installeren van virusscanners en wachtwoordbeveiliging.
- Meld storingen van beheerde werkplekken (computer of laptop) bij de afdeling ICT.

2.3 De fysieke werkplek / 'clean desk policy'

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 pc (windowstoets+L).
- Verwijder interne en vertrouwelijke documenten van het bureau 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-mailprogramma 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 of in de daarvoor bestemde beveiligde papiercontainer.

LET OP:
Als persoonsgegevens toegankelijk/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. Beveiligingsincidenten en mogelijke datalekken moeten, conform het protocol dataleken, worden gemeld via privacy@regiuscollege.nl.

2.4 Gebruik eigen devices

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor het Regius College worden uitgevoerd. Het Regius College is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school.

Voor 'eigen devices' ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:
- Beveilig het device met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode.
- Vergrendel het device bij het verlaten van de werkplek (windowstoets+L).
- Sla <u>persoonsgegevens</u> van het Regius College niet op het eigen device op; dit is niet toegestaan.
- Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot het Regius College als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden.
- Scheid (versleutelde)gegevens, anders dan persoonsgegevens, van het Regius College en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen device.

- Houd software up-to-date.
- 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.

2.5 Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal is niet meer weg te denken bij het Regius College. 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:

- Aanvragen van online onderwijsapplicaties en/of andere software loopt in alle gevallen via de afdeling ICT.
- Installeren van software wordt bij het Regius College 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 verwerkt worden.
- Een verwerkersovereenkomst wordt afgesloten met elke leverancier van (online)software, die in opdracht van het Regius College persoonsgegevens verwerkt.

2.6 Gebruik van e-mail en internet

Het Regius College stelt het gebruik van een e-mailsysteem en internet aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden.

- Medewerkers zijn op school beperkt gerechtigd bedrijfsmiddelen te gebruiken voor niet werkgerelateerd e-mail-, internet- en telefoonverkeer, mits dit niet storend is voor hun werkzaamheden.
- Tijdens het verzorgen van lessen zijn bedrijfsmiddelen alleen toegestaan voor activiteiten die rechtstreeks verband houden met die lessen.
- De communicatie met leerlingen en hun ouders dient zakelijk te zijn. Een medewerker doet geen uitspraken en/of toezeggingen waarvan de medewerker vooraf niet zeker weet of ze nagekomen kunnen worden. Bij twijfel overlegt een medewerker met zijn leidinggevende.
- 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.
- Het is niet toegestaan om
  - op internetsites 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
  - deel te nemen aan kansspelen.

2.7 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. Het Regius College verwacht van medewerkers dat zij:

- het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken) en websites;
- weten wat malware[2] is, het kunnen herkennen en weten hoe te handelen;
- terughoudend zijn met het online achterlaten van gegevens met betrekking tot het Regius College;
- controleren of er daadwerkelijk van een bekend én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes.

2.8 Sociale media

Sociale media is een verzamelnaam voor alle internettoepassingen die het mogelijk maken om informatie met elkaar te delen op een eenvoudige en vaak leuke manier. 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 social media (Instagram, YouTube, Facebook, Twitter enz). De essentie van sociale media is dat iemand er informatie deelt over zichzelf, over anderen of over een bepaald onderwerp.

Bij het Regius College gelden de volgende afspraken voor het gebruik van sociale media:

- Alles wat een medewerker schrijft of plaatst, is en blijft de verantwoordelijkheid van die medewerker. Plaats nooit berichten die het imago van collega's, leerlingen en/of het Regius College kunnen schaden. Bij twijfel geldt altijd: niet plaatsen. Medewerkers worden gezien als 'iemand van het Regius College' - ook als die medewerker een privémening verkondigt. Een medewerker dient na te gaan of communiceren op persoonlijke titel de juiste keuze is. Bij twijfel vraagt een medewerker advies aan zijn leidinggevende.
- Voor social media gelden dezelfde afspraken op het gebied van persvoorlichting en woordvoering als voor de traditionele media zoals krant en TV. Berichten en reacties op berichten uit naam van het Regius College worden dan ook alleen gedaan door het College van Bestuur of de sectordirecteuren, indien het hun sector betreft.
- Uiteraard respecteert het College van Bestuur de vrijheid van meningsuiting van medewerkers. Een medewerker dient zich te realiseren dat de persoonlijke mening over bepaalde zaken strijdig kan zijn met de belangen van het Regius College. Een medewerker dient zich ook te realiseren dat berichten niet alleen gelezen worden door vrienden en familie en dat wat men schrijft, blijvend is.
- Een medewerker geeft nooit vertrouwelijke informatie van of over collega's, leerlingen en/of het Regius College.

---

[2] *Malware is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Het woord is een samentrekking van het Engelse malicious software (kwaadaardige software, soms schadelijke software).*

2.9 Gebruik beeld- en geluidsmateriaal

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

- Het Regius College 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.

2.10 Wachtwoorden, tweeweg verificatie

- Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en devices (pc, laptop, telefoon) begint met een goed wachtwoord. Een lang wachtwoord of een 'wachtzin' is beter dan een kort, complex wachtwoord. Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Voor alle medewerkers is tweeweg verificatie verplicht voor onze cloudproducten (SOMtoday, Google omgeving en Afas).

2.11 Meldplicht Datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens de procedure meldplicht datalekken van het Regius College.

Beveiligingsincidenten en mogelijke datalekken worden altijd direct gemeld via privacy@regiuscollege.nl.

3. Controle gebruik bedrijfsmiddelen

Het Regius College handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:

- De Grondwet
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Wet Medezeggenschap Onderwijs (WMO)
- Burgerlijk Wetboek (BW)
- Wetboek van Strafrecht
- Cao VO

3.1 Voorwaarden voor controle

- De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. Het Regius College zal dan ook de controle en handhaving van deze regels conform de privacywetgeving en het algemene arbeidsrechtelijk kader 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 bestuur de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang.

- Het is het College van Bestuur in beginsel toegestaan de vastgelegde gegevens door het gebruik van bedrijfsmiddelen te analyseren ten behoeve van het onderzoeken van ongeoorloofd gedrag, indien er sprake is van een gerede verdenking of vermoeden van een ongeoorloofde handeling door één of meerdere medewerkers. Hierbij wordt ervan uitgegaan dat er een zwaarwichtig belang van het Regius College in het geding is en dat bij de uitvoering rekening wordt gehouden met de ernst van de gevolgen voor de betrokken medewerker(s) en de wijze waarop in zijn/hun privacy wordt voorzien.
- De betreffende gegevens worden bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen tegen een gebruiker noodzakelijk is.
- Het College van Bestuur behoudt zich het recht voor om het gebruik van bedrijfsmiddelen te beperken zoals de toegang tot bepaalde sites en telefoonnummers. Met name sites met, of nummers die toegang bieden tot pornografische, racistische, discriminerende of op entertainment gerichte inhoud kunnen worden geweerd.

3.2 Disciplinaire maatregelen

Bij het handelen in strijd met dit protocol of de algemeen geldende wettelijke regels, kan het bestuur van het Regius College, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen. Er worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

3.3 Rechten van medewerkers

- Medewerkers hebben het recht de over hem of haar geregistreerde data in te zien en/of hiervan een kopie te ontvangen.
- Medewerkers hebben het recht om feitelijk onjuiste gegevens in de geregistreerde data te (laten) verbeteren of aan te vullen.
- Medewerkers hebben het recht om de over hem of haar geregistreerde data, die niet (langer) ter zake doen of in strijd zijn met dit protocol of een wettelijk voorschrift, te laten verwijderen en/of te laten vernietigen.

Wij zullen binnen één maand van ontvangst van een verzoek reageren op welke wijze we gevolg hebben gegeven (of gaan geven) aan een verzoek. Echter, wanneer een verzoek heel complex is of wanneer het aantal ontvangen verzoeken heel groot is, kan deze termijn in uiterste gevallen met twee maanden worden verlengd. Ook hierover zullen we de betrokkene binnen één maand na ontvangst informeren.

4. Slotbepaling

Deze protocol kan, na instemming van de GMR, worden gewijzigd als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan werknemers bekend gemaakt. In gevallen waarin dit protocol niet voorziet, beslist het CvB.