REGLEMENT GEBRUIK INTERNET EN TELECOMMUNICATIE
HOGESCHOOL ROTTERDAM

Hogeschool Rotterdam biedt medewerkers en studenten de mogelijkheid gebruik te maken van de internet- en overige telecommunicatiemiddelen ten behoeve van hun werkzaamheden en studie. Aan het gebruik van deze door Hogeschool Rotterdam aangeboden faciliteiten zijn regels verbonden.

Dit Reglement stelt regels voor het gebruik van deze faciliteiten. Het reglement geldt voor alle medewerkers, studenten en gastgebruikers van Hogeschool Rotterdam. Voor elk van deze groepen gebruikers kunnen specifieke regels gelden.

Artikel 1. Begripsbepalingen

In dit Reglement wordt onder de volgende begrippen het volgende verstaan:

AVG: Algemene Verordening Gegevensbescherming

Beheerder: de directeur van de dienst Faciliteiten en Informatietechnologie (FIT).

College van Bestuur: het College van Bestuur van Hogeschool Rotterdam.

Datalek: een inbreuk op de beveiliging als bedoeld in artikel;4 lid 12 AVG; een inbreuk leidt, per ongeluk of op onrechtmatige wijze, tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
Directeur: de directeur van een Instituut of een Dienst van de HR.

Functionaris Gegevensbescherming (FG): de door de HR aangestelde functionaris als bedoeld in artikel 37 AVG die toezicht houdt op de toepassing en naleving van de Algemene Verordening Gegevensbescherming.

Gastgebruikers: degenen die met toestemming van Hogeschool Rotterdam gebruik maken van de in dit reglement bedoelde internet en telecommunicatievoorzieningen niet zijnde medewerkers en studenten.

Gebruikers: medewerkers, studenten en gastgebruikers.

HR: Hogeschool Rotterdam.

Internet en telecommunicatievoorzieningen: alle bekabelde en draadloze communicatie-, computer- en netwerkvoorzieningen binnen de HR waarmee datacommunicatie tot stand kan worden gebracht. Tot deze voorzieningen behoren in ieder geval toegang tot en gebruik van het netwerk van HR en alle daaraan gekoppelde apparatuur, bijbehorende software, en de verbindingen met andere netwerken, zoals internet, computer-, audiovisuele en overige ICT-voorzieningen in leslokalen en overige ruimten van de HR. Ook telefoon- en e-mailvoorzieningen maken deel uit van deze voorzieningen.

Medewerker(s): degene(n) die op arbeidsovereenkomst werkzaamheden verricht bij of ten behoeve van de HR alsook personeel niet in loondienst.

Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Register van verwerkingen: het register met de verwerkingsactiviteiten als bedoeld in artikel 30 AVG.

Social media: online communicatieplatformen die worden gebruikt om informatie te posten en met anderen te delen anders dan via e-mailverkeer.

Student(en): degene(n) die als student of extraneus staat/staan ingeschreven voor een opleiding bij de HR.

Systeembeheerder(s): de medewerker(s) die in het kader van beheerswerkzaamheden vanuit zijn/hun functie(s) beschikt/beschikken over nadere bevoegdheden binnen ICT-systemen.

Toegangscode: een gebruikers-/login-naam en wachtwoord (voor medewerkers tevens de bijbehorende authenticatiecode).

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Artikel 2. Reikwijdte, doel en uitgangspunten

1. Tenzij anders is bepaald of uit de aard van de bepalingen voortvloeit, is dit reglement van toepassing op medewerkers, studenten en gastgebruikers. Dit reglement is ook van toepassing op natuurlijke personen die gebruik maken van netwerkvoorzieningen van andere instellingen waarbij toegang wordt verkregen op basis van de inloggegevens van de HR (eduroam).
2. Dit reglement stelt regels voor het gebruik van internet en telecommunicatievoorzieningen.
3. Deze regels dienen in ieder geval de volgende doelen:
* systeem- en netwerkbeveiliging;
* bewaking van de netwerkintegriteit en -stabiliteit;
* bescherming van persoonsgegevens;
* bescherming van vertrouwelijke informatie;
* het tegengaan van discriminatie, seksuele intimidatie, bedreiging en geweld alsmede overige strafbare feiten;
* bescherming van de rechten van intellectuele eigendom van de HR en van derden;
* het tegengaan van misbruik, oneigenlijk en bovenmatig gebruik, en
* kostenbeheersing.

Artikel 3. Algemene bepalingen omtrent gebruik van de faciliteiten

1. De HR stelt internet en telecommunicatievoorzieningen (zoals openbare computers, tablets, telefoons, bekabelde en draadloze netwerkaansluitingen, e-mail en internettoegang, software, opslagcapaciteit, printers en elektronische leeromgevingen) beschikbaar aan gebruikers in verband met de uitvoering van werkzaamheden en studie.
2. Gebruikers gaan zorgvuldig om met de aan hen beschikbaar gestelde voorzieningen en laten apparatuur waarop zij zijn ingelogd niet zonder die te hebben vergrendeld ('gelockt') achter. Ingeval een medewerker de werkruimte verlaat, kan vergrendelen slechts achterwege blijven ingeval sprake is van kortdurende afwezigheid en afdoende toezicht door (een) collega('s) is gewaarborgd.
3. Beperkt privégebruik van de voorzieningen is toegestaan. Dit gebruik mag echter geen storende invloed hebben op de goede werking van het netwerk of andere ICT-faciliteiten van de HR en mag geen overlast veroorzaken bij anderen, of inbreuk maken op rechten van de HR of derden.
4. Het veranderen van instellingen in voorzieningen beschikbaar gesteld door de HR in de gebouwen en terreinen van de HR is niet toegestaan, tenzij daarvoor van de systeembeheerder schriftelijke toestemming is verkregen. Aan deze toestemming kunnen nadere voorwaarden worden verbonden.
5. Het aansluiten van eigen apparatuur en toepassingen op de faciliteiten binnen de HR is slechts toegestaan zolang dit gebruik voldoet aan de regels van dit reglement.
6. Gebruikers moeten de instructies die door of namens de HR worden gegeven voor het gebruik van de faciliteiten direct opvolgen.
7. De HR kan aan het gebruik van de voorzieningen aanvullende gebruiksregels en voorwaarden stellen.

Artikel 4. Toegangscode

1. De aan gebruikers toegekende toegangscode is strikt persoonlijk en mag niet worden gedeeld met anderen.
2. Gebruikers dienen zorgvuldig om te gaan met hun toegangscode. Zij zijn steeds persoonlijk verantwoordelijk voor het (verdere) gebruik dat daarvan wordt gemaakt en de gevolgen van dat gebruik.
3. Gebruikers nemen alle redelijke maatregelen ter beveiliging van hun toegangscode. Bij constatering van verlies of misbruik dienen zij de systeembeheerder daarvan direct op de hoogte te stellen.
4. Bij een redelijk vermoeden van misbruik kan de systeembeheerder het betrokken account direct ontoegankelijk (laten) maken.

Artikel 5. Niet toegestane handelingen

1. Ten aanzien van het gebruik van de voorzieningen zijn in ieder geval de volgende handelingen of gedragingen (dan wel nalaten) niet toegestaan:

a. handelingen die de integriteit, stabiliteit, continuïteit of behoorlijke werking van de voorzieningen ondermijnen;
b. zichzelf of een derde toegang verschaffen tot het account of gegevens van een andere gebruiker, tenzij dit gebeurt in verband met het uitoefenen van toezicht door de HR;
c. toegang (doen) verkrijgen tot programmabestanden van computersystemen of deze te (doen) wijzigen of te (doen) vernietigen, tenzij daarvoor uitdrukkelijk schriftelijke toestemming is verleend;
d. systeem- of toegangscodes van anderen te gebruiken of misbruiken;

e. toegang verschaffen voor zichzelf of voor een ander tot computer- of andere ICT-systemen, (e-mail)accounts of andere voorzieningen waarvoor niet uitdrukkelijk toegang is verleend;
f. zich bij het gebruik van de faciliteiten, in het bijzonder e-mail of social media, uitgeven voor een ander, bijvoorbeeld om daarmee bij een derde de schijn te wekken dat die ander de afzender van dat dataverkeer is;
g. voor een ander bestemd dataverkeer (waaronder e-mail) lezen, kopiëren, wijzigen of wissen, tenzij dit plaatsvindt in verband met het uitoefenen van toezicht door de HR;
h. opzettelijk, of door verwijtbaar handelen of nalaten computer-"virussen" op en via de voorzieningen te introduceren;
i. de door de HR in verband met de werkzaamheden en studie ter beschikking gestelde programmatuur, databestanden en documentatie te kopiëren voor dan wel ter inzage te geven of ter beschikking te stellen aan onbevoegden.

2.
Als in strijd met de gebruiksvoorwaarden wordt tevens aangemerkt:

a. het vanuit werkplekken, klaslokalen of overige ruimten en terreinen van de HR, dan wel met gebruikmaking van de voorzieningen elders, raadplegen van internetdiensten met een racistische, discriminerende of pornografische inhoud, tenzij een onderwijs- of onderzoeksopdracht dit aantoonbaar noodzakelijk maakt;
b. het (doen) genereren, verzenden of doorzenden van berichten met de onder a. bedoelde inhoud of van (seksueel) intimiderende inhoud of van berichten die aanzetten tot discriminatie, haat en/of geweld;
c. het (doen) versturen van ongevraagde berichten aan grote aantallen ontvangers tegelijk of het verspreiden van kwaadaardige software (zoals malware en ransomware);
d. filesharing- of streamingdiensten te gebruiken die dusdanig veel dataverkeer genereren dat dit een storende invloed heeft op de goede werking en beschikbaarheid van het netwerk of andere voorzieningen;
e. het gebruik van door de HR ten behoeve van de werkzaamheden en studie beschikbaar gestelde software in strijd met de licentievoorwaarden;
f. films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de medewerker of student weet of behoort te weten dat dit in strijd is met de auteursrechtelijke bepalingen;
g. films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden onder derden;
h. foto’s of ander beeldmateriaal van een ander waarvan kan worden vermoed dat dit auteursrechtelijk is beschermd zonder de uitdrukkelijke schriftelijke toestemming van die ander te gebruiken op websites of in werkstukken;
i. een ander dan in dit reglement bedoeld doen of laten dat bij of krachtens de wet strafbaar is gesteld.

Artikel 6. Informatiebeveiliging; melden van verwerkingen aan de FG

1. Gebruikers nemen bij het gebruik van de faciliteiten in verband met hun werkzaamheden en hun studie de HR-regels voor de informatiebeveiliging en de bescherming van persoonsgegevens in acht.
2. Van gebruikers wordt een zorgvuldige en proactieve houding verwacht om door de HR aan hen beschikbaar gestelde computers en andere apparatuur, zoals smartphones, tablets, adequaat te beveiligen. De door HR beschikbaar gestelde mobiele voorzieningen zoals laptops en telefoons dienen altijd te zijn voorzien van een wachtwoord of een ander vorm van beveiliging teneinde

onbevoegd gebruik en onbevoegde inzage tegen te gaan.3. Ingeval gebruikers met eigen apparatuur gebruik maken van de voorzieningen van de HR, dienen zij in ieder geval:
a. de eigen apparatuur te voorzien van een adequate virusscanner en firewall, en de software-instellingen geregeld te updaten;
b. onbevoegde kennisneming en onrechtmatige verwerking van persoonsgegevens tegen te gaan.
4. Studieresultaten worden uitsluitend verwerkt in en bekend gemaakt via het door de HR gehanteerde studentvolgsysteem (Osiris).
5. Studenten moeten zonder belemmeringen aan het onderwijs kunnen deelnemen en studievoortgang kunnen boeken zonder dat zij daarbij genoodzaakt zijn hun persoonsgegevens te delen via niet door de HR gefaciliteerde internet- en telecommunicatievoorzieningen.
6. Van elke geautomatiseerde verwerking van persoonsgegevens dient opgaaf te worden gedaan bij de beheerder van het verwerkingenregister, met gebruikmaking van het daarvoor bestemde formulier. Een verwerking behoeft de goedkeuring van de FG en wordt opgenomen in het verwerkingenregister van de hogeschool.
Toelichting: deze bepaling houdt de verplichting in om bij de aanleg van een (database)bestand met persoonsgegevens van de HR (bijvoorbeeld adressenlijsten van een groep studenten of medewerkers, of roosters met namen van studenten en/of docenten), opgaaf te doen door middel van een formulier waarmee een verwerking wordt aangemaakt.

Artikel 7. Beveiligen van persoonsgegevens; meldplicht datalekken

1. Bestanden met persoonsgegevens van gebruikers die met behulp van een internetverbinding (dus ook e-mailverkeer), opgeslagen op een opslagmedium (cd-rom, usb-stick e.d.) of anderszins via datacommunicatie (zoals een telefoon, tablet of smartwatch) naar buiten de HR worden gebracht, dienen steeds te zijn beveiligd met behulp van adequate encryptie (versleuteling), opdat onbevoegde kennisneming en onrechtmatige verwerking zo goed mogelijk worden tegengegaan.
2. Verwerking (zoals verzending en opslag) van persoonsgegevens en het delen van bestanden met persoonsgegevens in de ’cloud’ is niet toegestaan, tenzij verwerking plaatsvindt met behulp van door de HR in verband met de werkzaamheden en studie gefaciliteerde internet- en telecommunicatievoorzieningen als bedoeld in artikel 3 lid 1.
3. Gebruikers dienen zodra zij kennis hebben van een datalek, daarvan direct melding te maken bij het door de HR ingestelde Response Team Datalekken.
4. Datalekken die aan het Response Team in ieder geval moeten worden gemeld zijn:
a. verlies of diefstal van een telefoon, computer, laptop, tablet/phablet, usb-stick, cd-rom of een andersoortige gegevensdrager alsook formulieren en documenten met persoonsgegevens van de HR;
b. besmetting met malware, ransomeware of besmettingen van vergelijkbare aard;
c. inbraak door een hacker;
d. een calamiteit zoals brand in een datacentrum.

Artikel 8. Vertrouwelijke informatie

1. Indien gebruikers in verband met de uitvoering van hun werkzaamheden of studie toegang krijgen tot informatie die door de HR als vertrouwelijk is aangemerkt en waarvan zij weten althans behoren te weten dat die vertrouwelijk is, dienen zij die informatie ook als vertrouwelijk te behandelen.
2. Indien de HR met betrekking tot het waarborgen van de vertrouwelijkheid voorschriften heeft gegeven, dienen deze te worden gerespecteerd.
3. De HR-voorschriften voor verwerking (zoals verzending en opslag) van vertrouwelijke informatie in de ‘cloud’, dienen in acht te worden genomen.

Artikel 9. Gebruik van social media

1. Onverminderd het in het Social Media Protocol en de Gedrags- en integriteitscode van de HR alsmede het elders in dit reglement daaromtrent bepaalde, nemen gebruikers bij gebruik van social media de volgende voorschriften in acht.
2. Gebruik van social media die door de HR beschikbaar is gesteld (zoals Yammer), vindt niet anoniem plaats; medewerkers en studenten vermelden bij communicatie via social media steeds hun naam en functie dan wel dat zij als student bij de HR een opleiding volgen.
3. Het is zonder voorafgaande toestemming van de HR niet toegestaan persoonsgegevens zoals adres, woonplaats, telefoonnummer, foto's en andere privacygerelateerde informatie betreffende gebruikers te verwerken via social media die door de HR beschikbaar is gesteld.
4. Het is niet toegestaan om persoonsgegevens van gebruikers te verwerken op social media zoals privé-platforms (bijvoorbeeld Linkedin, Facebook, Hyves, Instagram, Twitter, e.d.) of privé-applicaties (zoals de berichtendiensten Whatsapp, Telegram, Snapchat e.d.), tenzij de betrokkene wiens gegevens het betreft daarvoor uitdrukkelijk schriftelijk toestemming heeft verleend en de belangen van de HR ook overigens door die verwerking niet worden geschaad.
5. Het Social Media Protocol voorziet in gedragsrichtlijnen en - aanbevelingen voor gebruik van social media; dit protocol maakt onderdeel uit van dit reglement en is als bijlage aangehecht.

Artikel 10. Algemeen toezicht en gericht onderzoek

1. De systeembeheerders voeren ten behoeve van systeem- en netwerkbeveiliging toezicht uit op het gebruik van de faciliteiten.
2. Middels algemeen toezicht dragen zij er onder verantwoordelijkheid van de beheerder zorg voor dat onbevoegden geen toegang krijgen tot systemen en netwerk, en dat gebruikers veilig gebruik kunnen maken van het netwerk.
3. Gegevens kunnen worden verzameld ten behoeve van controle op naleving van de regels. Deze gegevens zijn slechts toegankelijk voor de systeembeheerder die het aangaat. Deze gegevens kunnen met andere systeembeheerders geanonimiseerd worden gedeeld voor het nemen van technische maatregelen gericht op de systeem- en netwerkbeveiliging.
4. Komt uit het algemeen toezicht een redelijk vermoeden van misbruik of gebruik van de faciliteiten in strijd met dit reglement, dan wordt de desbetreffende gebruiker door of namens de directeur van de dienst die dan wel het instituut dat het aangaat, daarop bevraagd. De gebruiker wordt in de gelegenheid gesteld een nadere toelichting te geven.
5. De directeur die het aangaat kan vervolgens de beheerder verzoeken om gericht onderzoek uit te (laten) uitvoeren.
6. Gericht onderzoek richt zich op de verkeersgegevens van het gebruik van de voorzieningen, met name e-mail, social media en internet, en de netwerkveiligheid en -stabiliteit. In tweede instantie kan, indien daartoe aanleiding bestaat, de inhoud van het dataverkeer (berichten en bestanden) onderwerp van onderzoek zijn. De betrokkene wordt daarover geïnformeerd.
7. Indien daartoe aanleiding bestaat, kan de beheerder zelf tot gericht onderzoek besluiten; alsdan informeert de beheerder betrokkene en de directeur van het Instituut of de Dienst die het aangaat.
8. In afwijking van lid 5 en lid 7 vindt gericht onderzoek dat betrekking heeft op werknemers benoemd in de functie van bedrijfsarts, Functionaris Gegevensbescherming, vertrouwenspersoon, studentendecaan of medewerkers alsmede studenten die lid zijn van een medezeggenschapsorgaan, uitsluitend plaats in opdracht van het College van Bestuur.
9. De uitkomsten van het onderzoek worden op schrift gesteld en ter kennis gebracht van de directeur die het aangaat. De directeur informeert betrokkene zo spoedig mogelijk en stelt hem in de gelegenheid te worden gehoord. Van het horen wordt een verslag gemaakt.

10. Het informeren van betrokkene als bedoeld in het vorige lid kan indien de omstandigheden daartoe aanleiding geven worden uitgesteld indien het gericht onderzoek daardoor ernstig zou worden gehinderd.
11. De beheerder kan bij wijze van ordemaatregel de gebruiker zodra de omstandigheden daartoe aanleiding geven een tijdelijke beperking van de toegang tot en het gebruik van de faciliteiten opleggen.
12. In aanvulling op het in dit artikel met betrekking tot gericht onderzoek bepaalde en onverminderd lid 8, kan de manager Beleid Ontwikkeling en Implementatie (BOI) van de dienst FIT (of diens plaatsvervanger) op verzoek van de directeur die het aangaat toegang verlenen tot het e-mailaccount van een medewerker die gedurende langere tijd anders dan vanwege vakantie- of kortstondig ziekteverlof niet in de gelegenheid is of weigert zijn werkzaamheden uit te voeren. Toegang wordt verleend indien dat naar het oordeel van de directeur noodzakelijk is voor de goede voortgang van de bedrijfsvoering. De manager BOI stelt de Functionaris Gegevensbescherming op de hoogte van de verleende toestemming.
13. Raadpleging van het e-mailaccount vindt slechts plaats in aanwezigheid van een systeembeheerder. Wordt in het e-mailaccount privémail aangetroffen, dan wordt deze ongelezen in een aparte bestandmap geplaatst.
14. Het bepaalde in de leden 12 en 13 is ook van toepassing op de medewerker die uit dienst is.

Artikel 11. Treffen van maatregelen

1. Indien een medewerker of student in strijd met dit reglement handelt of aanwijzingen van de systeembeheerder weigert op te volgen, kan de directeur die het aangaat, afhankelijk van de aard en de ernst van de overtreding, maatregelen treffen.
2. Indien een gastgebruiker in strijd met dit reglement handelt of aanwijzingen van de systeembeheerder weigert op te volgen, kan de beheerder dan wel de directeur die het aangaat, afhankelijk van de aard en de ernst van de overtreding, maatregelen treffen die hem geraden voorkomen.
3. Indien de uitkomsten van een gericht onderzoek als bedoeld in artikel 10 daartoe aanleiding geven, kan de directeur die het aangaat jegens betrokkene, afhankelijk van de aard en de ernst van de overtreding, maatregelen treffen. Is betrokkene in het kader van een gericht onderzoek nog niet gehoord, dan vindt het horen alsnog plaats alvorens tot een maatregel wordt overgegaan.

Artikel 12. Inhoud van op te leggen maatregelen

1. Ingeval uit gericht onderzoek blijkt dat sprake is van onjuist gebruik van de voorzieningen door een medewerker, kan de directeur die het aangaat de volgende in de cao-hbo bedoelde disciplinaire maatregelen (hoofdstuk P-4) nemen: schriftelijke berisping, overplaatsing, schorsing, ontslag op staande voet. Het opleggen van een maatregel als hier bedoeld verloopt via de daarvoor in de cao-hbo aangemerkte procedure (hoofdstuk P-2) en behoeft de goedkeuring van het College van Bestuur.
2. Jegens studenten kan in gevallen als in het eerste lid bedoeld de directeur die het aangaat een ordemaatregel opleggen als bedoeld in (artikel 7.57h van) de Wet op het hoger onderwijs en wetenschappelijk onderzoek, te weten ontzegging van de toegang tot de gebouwen en terreinen van de HR voor de duur van ten hoogste één jaar. In ernstige gevallen kan het College van Bestuur de toegang tot de HR definitief ontzeggen.
3. Bij overtreding van de bepalingen van dit reglement door gastgebruikers zijn denkbare maatregelen (al dan niet tijdelijke) ontzegging van gebruik en toegang tot de voorzieningen of, als meest vergaande maatregel, onmiddellijke beëindiging van de samenwerking, onverminderd het recht van HR om alle schade samenhangend met en voortvloeiend uit de overtreding te verhalen.

4. Bij het opleggen van een maatregel worden de procedures als bedoeld in artikel 4.5 van de hogeschoolgids in acht genomen.

Artikel 13. Rechtsbescherming

1. De medewerker aan wie een disciplinaire maatregel is opgelegd, kan binnen zes weken gerekend vanaf de dag na die waarop het besluit is verzonden, beroep instellen bij de Commissie van beroep personeel als bedoeld in (Hoofdstuk S van) de cao-hbo.
2. De student aan wie een ordemaatregel is opgelegd, kan binnen zes weken gerekend vanaf de dag na die waarop het besluit is verzonden, bezwaar maken bij de Geschillenadviescommissie.

Artikel 14. Inwerkingtreding en slotbepalingen

1. Dit reglement treedt in werking op 25 mei 2018 en vervangt het laatstelijk voor die datum vastgestelde reglement.
2. Dit reglement wordt door het College van Bestuur vastgesteld en gewijzigd. De Centrale Medezeggenschapsraad wordt in de gelegenheid gesteld op dit reglement het adviesrecht uit te oefenen.
3. In gevallen waarin dit reglement niet voorziet, beslist het College van Bestuur.

Bijlage: Social Media Protocol Hogeschool Rotterdam als laatstelijk vastgesteld.