# Acceptable Use Policy

## Reglement voor ICT- en internetgebruik voor studenten UM.

Versie 2.0

17 november 2020

| Versie | Status | Datum | Door |
|---|---|---|---|
| **1.1** | Concept | 4 augustus 2020 | CISO |
| **1.2** | Concept | 5 augustus 2020 | Privacy-team / UM-SOC |
| | | | |
| | | | |
| | | | |
| **1.3** | Instemming | 22 september 2021 | Universiteitsraad |
| **2.0** | Vastgesteld | 17 november 2020 | College van Bestuur |
| | | | |
| | | | |

Inhoudsopgave

# Preambule

In deze Acceptable Use Policy (AUP) kun je lezen welke reglementen voor ICT- en internetgebruik het College van Bestuur van de UM heeft vastgesteld voor haar studenten. Een AUP is noodzakelijk om aan de studenten duidelijk te maken hoe zij de ICT-voorzieningen van de UM kunnen gebruiken bij hun studie, zonder dat ze daarbij (wettelijke) regels en richtlijnen overtreden en zonder dat zij de veiligheid van de digitale systemen van de UM in gevaar brengen. Maar vooral ook zonder dat ze de veiligheid van andere gebruikers in gevaar brengen. Tenslotte zorgen de afspraken in de AUP er ook voor dat je rechten als student worden gerespecteerd.
De AUP wordt daarom aan iedere student ter beschikking gesteld. Van alle gebruikers van de ICT-faciliteiten van de UM wordt verwacht dat ze bekend zijn met de UM-reglementen en de wet en dat ze vooral ook hun "gezond verstand" gebruiken.

De gebruikers binnen de UM vormen een afspiegeling van de maatschappij. Dit betekent dat gebruikers vergissingen of fouten kunnen maken en het is zelfs denkbaar dat moedwillig ongewenste handelingen gepleegd worden. Geen enkel reglement is hier tegen bestand.
Het is natuurlijk ook denkbaar dat je als gebruiker ondanks je voorzorgsmaatregelen toch slachtoffer wordt van een phishing aanval of een virus- of malware infectie.
De nadrukkelijke bedoeling van de AUP is de verwachtingen tussen gebruikers onderling en tussen gebruikers en systeembeheerders te verduidelijken en een kader te bieden om daar onderling over te kunnen communiceren. We vragen je dan ook om dit in een open sfeer te doen. De kans op fouten, vergissingen en misverstanden wordt zo verkleind.

Voor gevallen van ongewenst gedrag voorziet de AUP in maatregelen. In de regel zal het gaan om een waarschuwing waarin wordt uitgelegd waarom onderhavig gedrag ongewenst is en wat de consequenties van (herhaling) van dat gedrag zijn. Niet uitgesloten is dat zich gevallen voordoen waarin de ernst van de situatie naar het oordeel van het CvB om een strenger ingrijpen vraagt en niet kan worden volstaan met een waarschuwing en een zwaardere sanctie gepast is.
De gebruiker krijgt in alle gevallen de gelegenheid om diens kant van het verhaal naar voren te brengen: hoor en wederhoor dus.
Juridisch taalgebruik is in een AUP onvermijdelijk. Een reglement moet namelijk maar voor één uitleg vatbaar zijn. Twijfel je over de afspraken in deze AUP, dan kun je altijd aan je studiebegeleider of aan de Servicedesk van ICTS vragen hoe in een bepaalde situatie te handelen.

## Inleiding

De Universiteit Maastricht (UM, hierna: de Instelling), biedt aan de eigen studenten en aan bezoekende studenten, extranei en alumni (hierna: Studenten) de mogelijkheid om diverse ICT-faciliteiten, zoals internetverbindingen, apparatuur en applicaties, te gebruiken (hierna samen: de Faciliteiten). Zo hebben studenten binnen de gebouwen van de Instelling de mogelijkheid om internet te gebruiken ten behoeve van de studie. Tevens worden aan studenten voor persoonlijk gebruik een instellingsgebonden e-mailbox, een digitale leeromgeving en overige faciliteiten, zoals opslag van bestanden, beschikbaar gesteld, ten behoeve van de studie en alumni activiteiten.

Aan het gebruik van de Faciliteiten zijn regels verbonden, in het kader van de informatieveiligheid, beschikbaarheid, rechten van de Instelling en eventuele derden en een goede gang van zaken in de gebouwen en op de terreinen van de Instelling. Deze regels zijn in dit ICT- en internetreglement voor studenten (hierna: het Reglement), opgenomen. Deze regels zijn van toepassing op studenten van de Instelling en bezoekende studenten. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT- en internetgebruik en de privacy van studenten.

Om te controleren of de Faciliteiten niet worden gebruikt op een manier die in strijd is met de regels of geldende wetgeving en om te zorgen dat het netwerk, de apparatuur en de applicaties altijd veilig zijn en niet overbelast worden, kan de Instelling het gebruik van de Faciliteiten monitoren op de manieren zoals beschreven in dit Reglement.

Het College van Bestuur heeft dit reglement vastgesteld op 17 november 2020. Omdat het Reglement voorziet in een verwerking van persoonsgegevens en controle op gedrag van studenten en de regeling rechten en plichten bevat voor studenten, is de Universiteitsraad van de Instelling instemming plichtig. De Universiteitsraad heeft op 22 september 2021 ingestemd met de inhoud van dit Reglement.

# 1. Gebruik van de Faciliteiten

Computer- en netwerkfaciliteiten (zoals openbare computers, draadloze en/of bedrade netwerkaansluitingen, opslagcapaciteit, printers en elektronische leeromgevingen) worden aan de student beschikbaar gesteld ten behoeve van de studie, onder meer voor het kunnen maken van opdrachten, verslagen en scripties, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten en medestudenten.

Het gebruik van eigen apparatuur en toepassingen op de Faciliteiten van de Instelling is toegestaan, zolang dit gebruik voldoet aan de regels van dit Reglement. Het veranderen van instellingen in apparatuur en toepassingen beschikbaar gesteld door de Instelling is alleen toegestaan met aparte toestemming van het systeembeheer. Het aansluiten van eigen netwerkapparatuur met als doel om de bedrade of draadloze netwerkaansluitingen van de Instelling te delen met anderen is altijd verboden, behalve in de privé woonruimte van studenten.

Dit Reglement geldt ook indien u als gast gebruik maakt van netwerkvoorzieningen van andere instellingen, waarbij toegang wordt verkregen op basis van de inloggegevens van de eigen Instelling (Eduroam).

Bepaalde Faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en wachtwoord, mogelijk aangevuld met een authenticatiemiddel zoals smartcard of mobiele telefoon. Deze zijn persoonsgebonden en mogen niet met anderen worden gedeeld. Het systeembeheer kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten, zoals nader geformuleerd in het Informatiebeveiligingsbeleid. Bij een vermoeden van misbruik van een wachtwoord of authenticatiemiddel kan het systeembeheer per direct het betreffende account ontoegankelijk maken.

## 1.1. Beveiliging door de Instelling en de student

De Instelling neemt informatiebeveiliging serieus. Zij hanteert dan ook een streng beveiligingsbeleid en neemt adequate technische en organisatorische maatregelen om de infrastructuur te beveiligen tegen verlies, diefstal, criminele activiteiten, verlies van vertrouwelijkheid, schending van privacy rechten en schending van intellectuele eigendomsrechten.

Natuurlijk is een perfecte beveiliging onmogelijk. Daarom verwacht de Instelling ook van studenten een proactieve houding en serieuze stappen om de eigen computer en andere apparatuur (zoals smartphones of tablets) adequaat te beveiligen. Zo is de student altijd zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens.

In het bijzonder dient de student, indien met eigen apparatuur gebruik wordt gemaakt van een netwerkaansluiting van de Instelling, in het kader van beveiliging:

- deze apparatuur te voorzien van een adequate virusscanner en firewall;
- onrechtmatige toegang tot systemen van de Instelling te voorkomen door moeilijk te raden wachtwoorden en/of pincodes te gebruiken;
- deze apparatuur up-to-date te houden wat betreft operating systeem en software-instellingen;
- versleuteling toe te passen op het operating systeem en de opgeslagen gegevens.

Het UM Informatiebeveiligingsbeleid en nadere uitleg over beveiliging en beveiligingsmaatregelen zijn opgenomen op de beveiligingspagina's van de UM:
https://www.maastrichtuniversity.nl/informatiebeveiliging.
Voor specifieke diensten en voorzieningen kunnen specifieke reglementen, afspraken of werkinstructies van toepassing zijn. Deze worden afzonderlijk gecommuniceerd.
Bij twijfel over afspraken, richtlijnen, maatregelen etc. kunt u navraag doen bij Servicedesk ICTS of bij systeembeheer.

## 1.2. Privégebruik en overlast

Hoewel de Faciliteiten bedoeld zijn voor gebruik ten behoeve van de studie, is privégebruik in beperkte mate toegestaan. Gebruik (privé of ten behoeve van studie) mag niet illegaal of storend voor de goede orde bij de Instelling zijn en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van de Instelling of derden of de integriteit en de veiligheid van het netwerk aantasten.

Voor zover het gebruik geen onderdeel uitmaakt van een studieopdracht wordt onder illegaal, storend en/of overlast veroorzakend gebruik in ieder geval verstaan:

- het in openbare ruimtes raadplegen van internetdiensten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud of het verzenden van berichten met een dergelijke inhoud;
- het verzenden van berichten met een (seksueel) intimiderende inhoud of van berichten die blijk geven van of (kunnen) aanzetten tot discriminatie, haat en/of geweld;
- het versturen van berichten aan grote aantallen ontvangers tegelijk, het versturen van kettingbrieven en phishing-mails of het verspreiden van kwaadaardige software zoals virussen, wormen, Trojaanse paarden en spyware;
- filesharing- of streamingdiensten (zoals internetradio of Uitzending gemist) te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de Faciliteiten kan aantasten;
- films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de student weet/moet weten dat dit in strijd met auteursrechten is;
- films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

Het gebruik van de Faciliteiten ten behoeve van eigen commerciële activiteiten is uitsluitend toegestaan, wanneer de Instelling hiervoor schriftelijk toestemming heeft verleend.

Het gebruik van UM VPN faciliteiten valt volledig onder de regeling van deze AUP, ongeacht het netwerk en het werkstation van waaruit de student de VPN sessie heeft opgestart.
Studenten die in hun woonruimte gebruik maken van een netwerkfaciliteit van de Instelling (zoals in UM Guesthouse locaties) worden aldaar geen beperkingen opgelegd aan het gebruik, behoudens voor zover noodzakelijk om de integriteit en de veiligheid van het netwerk te kunnen bewaren, of om de gevolgen van congestie te beperken. Indien de Instelling ingrijpt om de gevolgen van congestie te beperken, zullen gelijke soorten verkeer gelijk worden behandeld. De overige bepalingen in dit Reglement zijn onverkort van toepassing voor studenten-gebruikers die in hun woonruimte gebruik maken van een netwerkfaciliteit van de Instelling.

## 1.3. Intellectueel eigendom en vertrouwelijke informatie

De student maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling en derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen de Instelling.

De zeggenschap over de informatie van de Instelling berust bij Instelling. De student heeft geen zelfstandige zeggenschap over de informatie behalve als hem/haar dat expliciet is toegekend door de Instelling

Het is de student niet toegestaan om grote hoeveelheden artikelen uit de bestanden van de digitale bibliotheek te downloaden of substantiële delen van de bestanden of databases in de digitale bibliotheek systematisch te kopiëren.

Indien de student in het kader van zijn studie of het uitvoeren van taken voor de Instelling toegang krijgt tot vertrouwelijke informatie of privacygevoelige informatie, dient de student die informatie strikt vertrouwelijk te behandelen.

De student besteedt bijzondere aandacht aan het treffen van maatregelen, zoals in dit Reglement genoemd, indien in het kader van het uitvoeren van deze taken de verwerking van vertrouwelijke informatie buiten de Instelling noodzakelijk is zoals via e-mail, in niet instellingsgebonden cloud-toepassingen, op externe opslagmedia of eigen apparatuur (USB-gegevensdragers, tablets, etc.). De student dient kopieën van instellingsdata veilig op te slaan, overeenkomstig de aard van de gegevens, en regelmatig reservekopieën te maken van deze data op opslagfaciliteiten van de Instelling.

Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten nadere voorschriften heeft opgesteld, dient de student deze stipt op te volgen.

# 2. Controle door de Instelling

De Instelling controleert de naleving van dit Reglement. De Instelling handelt bij de controle op het gebruik van de Faciliteiten binnen de geldende wet- en regelgeving.

De Instelling streeft in het kader van de controle en handhaving van dit Reglement naar maatregelen, die inzage in privacygevoelige informatie of persoonsgegevens van individuele studenten zo veel mogelijk beperken. De Instelling zal daarbij uitgaan van de juiste balans tussen verantwoord gebruik van de Faciliteiten en de bescherming van de privacy van studenten. Zij zal, waar mogelijk, slechts geautomatiseerd controleren of filteren, zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

## 2.1. Voorwaarden voor controle

Controle van gebruik van de Faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit Reglement ten behoeve van de goede orde binnen de Instelling, de bewaking van de integriteit en de veiligheid van het netwerk, de computerfaciliteiten van de Instelling, haar studenten en medewerkers of derden.
Verboden gebruik van de Faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

Ten behoeve van deze controle worden geautomatiseerd gegevens verzameld (gelogd). Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens, die niet herleidbaar zijn tot identificeerbare personen. De gegevens, die uit een dergelijke controle voortkomen, zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten, zoals een blokkade van de toegang tot een bepaalde dienst of het beperken van de mogelijkheden van het apparaat in kwestie om het netwerk te kunnen gebruiken.

In het bijzonder kan bij overlast, veroorzaakt door apparatuur van studenten, worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de student vooraf gewaarschuwd, zodat hij de gelegenheid heeft de overlast te staken. Wanneer dit wegens de vereiste spoed niet voorafgaand aan het nemen van de maatregel mogelijk is, wordt de student zo snel mogelijk na het nemen van de maatregel geïnformeerd.

Bij vermoedens van overtreding van de regels kan gedurende een vastgestelde (korte) periode, gerichte controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het

gebruik van de Faciliteiten. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats. De procedure bij gericht onderzoek, wordt hieronder in hoofdstuk 2.3 beschreven.

De Instelling houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud onverkort aan de Algemene verordening gegevensbescherming (AVG) en andere relevante wet- en regelgeving. In het bijzonder beveiligt de Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

Persoonsgegevens, die zijn vastgelegd in het kader van toezicht en controle, worden bewaard voor een zo kort mogelijke periode. Enkel indien er een redelijk vermoeden bestaat van onrechtmatig gebruik kan deze periode worden verlengd. Zodra een onderzoek is afgerond en niet leidt tot maatregelen tegenover een betrokkene, worden de gegevens verwijderd.

## 2.2. Uitvoering van de controle

Om controle uit te kunnen voeren op de naleving van dit Reglement, kan de Instelling enkele specifieke maatregelen treffen. Zo vindt de controle op het uitlekken van vertrouwelijke informatie, waartoe de student in het kader van zijn studie of het uitvoeren van taken voor de Instelling toegang heeft, plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.

Daarnaast wordt de controle in het kader van kosten- en capaciteitsbeheersing beperkt tot het op basis van verkeersgegevens nagaan van de bronnen van kosten of capaciteitsvraag (zoals de adressen van internetradio en videosites). Als deze websites tot grote kosten of overlast leiden, worden zij geblokkeerd of afgeknepen, zonder daarbij de vertrouwelijkheid van de inhoud van de communicatie te schenden;

De afdeling ICT en de systeembeheerder(s) zijn aan geheimhouding gebonden als men in het kader van de controle op dit Reglement 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 de Instelling worden in het kader van de controle op dit Reglement de nodige maatregelen getroffen, zodat persoonsgegevens, gelet op de doeleinden waarvoor zij verwerkt worden, juist en nauwkeurig zijn.

Door de Instelling worden in het kader van de controle op dit Regelement passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

## 2.3. Procedure bij gericht onderzoek

Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende de student worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die student.

Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van het College van Bestuur, waarbij wordt mede wordt vastgelegd wie van het onderzoek en eventueel van de vastgelegde resultaten op de hoogte wordt gesteld. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de Faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de Instelling na aparte opdracht van

het CvB overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

Gericht onderzoek naar de beveiliging of integriteit van randapparatuur mag in afwijking hiervan door het systeembeheer worden uitgevoerd op basis van concrete aanwijzingen, zonder aparte toestemming. De resultaten van dit onderzoek worden alleen gedeeld met de student met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaling zal de procedure uit de vorige 2 paragrafen worden gevolgd.

De student wordt zo spoedig mogelijk schriftelijk geïnformeerd namens het CvB over de aanleiding, de uitvoering en het resultaat van het onderzoek. De student wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou schaden of hier een sterk vermoeden van is.

Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van de student als de student daarvoor zijn toestemming heeft gegeven. Toegang tot accounts zonder deze toestemming is slechts toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van dit Reglement, zoals nader bepaald in dit artikel. De student zal in dat geval achteraf worden geïnformeerd.

## 3. Consequenties van overtreding van dit Reglement

Bij handelen in strijd met dit Reglement of de algemeen geldende wetgeving bij het gebruik van de Faciliteiten, kan het bestuur van de Instelling, afhankelijk van de aard en de ernst van de overtreding, maatregelen treffen.

Hieronder vallen een waarschuwing, berisping, een tijdelijke afsluiting of beperking van de Faciliteiten (maximaal een jaar) en in extreme gevallen een beëindiging van de inschrijving als student.

Maatregelen (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde weg uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade. In geval van een waarschuwing op basis van een geautomatiseerde verwerking krijgt de student gelegenheid zijn zienswijze naar voren te brengen. Verder worden geen maatregelen getroffen anders dan bij herhaling van geconstateerde feiten zoals beschreven in de volgende paragraaf.

Al dan niet tijdelijke beperkingen in de toegang tot bepaalde Faciliteiten of andere ordemaatregelen kunnen worden opgelegd indien gehandeld wordt in strijd met dit Reglement en daarvoor al eerder een waarschuwing is uitgevaardigd met daarin opgenomen de aard van de geconstateerde handelingen en de consequenties van een eventuele herhaling. De student wordt daarvoor eerst in de gelegenheid gesteld naar aanleiding van de genoemde waarschuwing zijn zienswijze naar voren te brengen.

In afwijking van het voorgaande is het mogelijk dat de Instelling bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende faciliteit invoert. Deze blokkade zal maximaal een week worden gehandhaafd of korter als de oorzaak naar tevredenheid van het systeembeheer is weggenomen. Indien na een week geen verbetering is geconstateerd door het systeembeheer, kan het systeembeheer besluiten tot een langere blokkade. Bij herhaling van de oorzaak kunnen aanvullende maatregelen worden genomen.

Indien er strafbare feiten worden geconstateerd die vallen onder de Wet Computercriminaliteit, zal de Instelling aangifte doen.

## 4. Rechten van de student met betrekking tot persoonsgegevens

De student heeft alle in de AVG opgenomen rechten mbt de verwerking van persoonsgegevens, conform vastgelegd in het privacy statement van de UM.

De student heeft daarnaast het recht op een menselijke blik bij besluiten op basis van automatisch verwerkte gegevens.

## 5. Slotbepalingen

Dit Reglement kan door het bestuur worden herzien. Wijzigingen worden bij voorkeur bij het begin van een formele studieperiode (september of februari) doorgevoerd, behalve in dringende gevallen of wanneer de Instelling door omstandigheden van buitenaf gedwongen is tot een tussentijdse/afwijkende datum van invoering. In alle gevallen zullen studenten hierover tijdig worden geïnformeerd.

Wijzigingen worden alleen ingevoerd nadat de Universiteitsraad om voorafgaand advies is gevraagd. Het College van Bestuur zal feedback van studenten in overweging nemen alvorens de wijzigingen in te voeren.

In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur.

Vastgesteld door het CvB van de Universiteit Maastricht d.d.: 17 november 2020
Instemming door de Universiteitsraad d.d.: 22 september 2021

**Bronvermelding:**