UNIVERSITEIT VAN AMSTERDAM

REGELS VOOR VERANTWOORD GEBRUIK VAN ICT-FACILITEITEN VOOR STUDENTEN AAN DE UNIVERSITEIT VAN AMSTERDAM

Vastgesteld bij besluit nr. 2018-068316 van het College van Bestuur van 25 september 2018

Basis voor Regels voor verantwoord gebruik van ICT-faciliteiten

De Universiteit van Amsterdam (hierna: de ***"UvA")*** biedt aan de eigen studenten en aan bezoekende studenten de mogelijkheid internet en ICT-middelen te gebruiken ten behoeve van de studie. Daarbij worden onder meer een instellingsgebonden mailbox en mogelijkheden tot opslag van bestanden en persoonlijke studiegegevens.

Aan het gebruik van deze faciliteiten zijn regels verbonden. In het kader van de goede gang van zaken in de gebouwen en op de terreinen van de UvA.
Met deze Regels voor verantwoord gebruik van ICT-faciliteiten (hierna: Reglement) wil de UvA regels stellen omtrent het gewenst gebruik van haar ICT-faciliteiten. Het streven daarbij is een goede balans aan te brengen tussen het inzetten van ICT-faciliteiten ten behoeve van de studie aan ene kant en het verantwoord en veilig gebruik van de ICT-faciliteiten en de privacy van de student aan de andere kant. De missie van de UvA is academisch onderwijs verzorgen voor de voorhoede van morgen, baanbrekend (fundamenteel) wetenschappelijk onderzoek verrichten en dit vertalen naar relevante maatschappelijke toepassingen. Het verantwoord gebruik van de ICT-faciliteiten ondersteunt medewerkers en studenten bij het realiseren van deze missie, binnen een instelling waarbij de vrijheid van handelen van medewerkers en studenten een groot goed is.

Dit Reglement treedt in werking op 25 september 2018 na instemming met dit Reglement van de Centrale Studentenraad (ex art. 27(1)(d) WOR) d.d. 05-07-2018.

Artikel 1. Uitgangspunten

1.1. Het Reglement stelt regels ten aanzien van het gebruik van internet en ICT-faciliteiten door studenten van de UvA. Doel van deze regels is de goede orde te bepalen ten aanzien van:
- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
- tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
- bescherming van persoonsgegevens;
- bescherming van vertrouwelijke informatie;
- bescherming van de intellectuele eigendomsrechten en het respecteren van licentieafspraken;
- kosten- en capaciteitsbeheersing.

1.2 Beperkt privégebruik van de internet en ICT- faciliteiten is toegestaan voor zover het niet storend is voor de goede orde bij de UvA en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van de UvA of derden of een storende invloed hebben op de goede werking, waaronder de beschikbaarheid, van het netwerk of andere ICT-faciliteiten.

1.3 Dit Reglement geldt voor iedereen die valt binnen de categorie 'Studenten'[1]. Dit Reglement is niet van toepassing op natuurlijke personen op wie het 'Reglement gebruik internet en ICT-faciliteiten voor medewerkers aan de Universiteit van Amsterdam' van toepassing is.

1.4 Dit Reglement is ook van toepassing indien gebruik wordt gemaakt van netwerkvoorzieningen van andere instellingen waarbij toegang wordt verkregen op basis van de inloggegevens van de UvA (eduroam).

[1] Het betreft hier zowel studenten die bij de UvA zijn ingeschreven en bezoekende studenten.

1.5 De UvA streeft in het kader van handhaving van dit Reglement naar maatregelen die inzage in persoonsgegevens van individuele studenten zo veel mogelijk beperken. De UvA zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

Artikel 2. Intellectueel eigendom en vertrouwelijke informatie

2.1 De student maakt geen inbreuk op de intellectuele eigendomsrechten van de UvA en derden en respecteert licentie afspraken.
2.2 De zeggenschap over de informatie van de UvA berust bij UvA. De student heeft geen zelfstandige zeggenschap of beschikkingsbevoegdheid over eigendom van de UvA behalve als hem dat expliciet is toegekend.
2.3 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.[2]
2.4. Indien de student in het kader van zijn studie of het uitvoeren van taken voor de UvA toegang krijgt tot vertrouwelijke informatie of privacy gevoelige informatie waaronder persoons-gegevens, dient de student die informatie op basis van de privacyregels strikt vertrouwelijk te behandelen.
2.5 De student besteedt bijzondere aandacht aan het treffen van veiligheidsmaatregelen 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 client-apparatuur (USB-apparaten, Tablets, etc.).
2.6 Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten voorschriften heeft opgesteld dient de student deze stipt op te volgen.

Artikel 3. Gebruik van ICT-faciliteiten

3.1. De ICT faciliteiten, zoals studiecentra faciliteiten, draadloze en netwerkaansluitingen, e-mail en internettoegang, opslagcapaciteit, printers en elektronische leeromgevingen, worden aan de student beschikbaar gesteld ten behoeve van de studie, onder meer voor het maken van opdrachten, verslagen en scripties, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten en medestudenten.
3.2. De student dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik daarvan kan de UvA per direct het betrokken account ontoegankelijk maken.
3.3 Ten aanzien van het gebruik van de ICT faciliteiten is het de student met name niet toegestaan:
a. zich toegang (trachten) te verschaffen tot gegevens van andere gebruikers en tot programmabestanden van computersystemen of deze te wijzigen of te vernietigen, behoudens uitdrukkelijk daartoe verleende verifieerbare toestemming;
b. zich toegang (trachten) te verschaffen tot computersystemen voor zover dit systemen betreft waarvoor geen expliciete toegangsmogelijkheid voor de student is gecreëerd;
c. acties te ondernemen die de integriteit en continuïteit van de ICT faciliteiten ondermijnen;
d. onbevoegde pogingen te ondernemen voor de ICT faciliteiten hogere privileges te bemachtigen dan de toegekende privileges;
e. onbevoegde pogingen te ondernemen om systeem- of gebruikers-autorisatiecodes (zoals wachtwoorden) op enigerlei wijze en in enigerlei vorm te bemachtigen;

[2] Dit artikel veronderstelt dat er auteursrechtelijke beperkingen zijn op de bestanden in de digitale bibliotheek. Gezien de ontwikkeling naar ‘open access’ wordt deze beperking minder relevant.

f. voor anderen bestemde (e-mail) berichten te lezen, kopiëren, wijzigen of uit te wissen;
g. de door de UvA ter beschikking gestelde programmatuur, databestanden en documentatie te kopiëren of ter beschikking te stellen aan derden, behoudens daartoe verleende schriftelijke toestemming;
h. opzettelijk, of door verwijtbaar handelen of nalaten computer-"malware"[3] (of andere kwaadaardige software) op en via de ICT-faciliteiten te introduceren.

3.4 Het installeren van software op de ICT-faciliteiten van de UvA is niet toegestaan zonder toestemming van ICTS.

3.5 Het aansluiten van servers en actieve netwerkcomponenten op het UvAnetwerk (zoals access points en routers is niet toegestaan zonder toestemming van ICTS.

3.6 Het aansluiten van eigen apparatuur (zoals laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. ICTS kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging.

3.7 Het opslaan van privébestanden of -informatie op systemen van de UvA is toegestaan, mits dit niet leidt tot overbelasting van de opslagcapaciteit van deze systemen of een verstoring van de goede orde op de werkvloer. De UvA is echter niet verplicht van dergelijke bestanden of informatie reservekopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen.

Artikel 4. Beveiliging door de UvA én de student

4.1 De UvA hanteert een informatiebeveiligingsbeleid 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.

4.2 De UvA verwacht ook van studenten een verantwoordelijke en proactieve houding om de eigen computer en andere apparatuur (zoals smartphones of tablets) adequaat te beveiligen. De student is te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens.
Indien de student met eigen apparatuur gebruikt maakt van de instellingsfaciliteiten, is het in het kader van het goed beheer van de eigen apparatuur raadzaam om onder meer:
- deze apparatuur te voorzien van een adequate virusscanner en firewall;
- deze apparatuur up-to-date te houden wat betreft software-instellingen;
- regelmatig reservekopieën te maken van alle relevante data en kopieën van instellingsdata veilig op te slaan.

Artikel 5. Privégebruik en overlast

5.1 Privégebruik van de internet en ICT-faciliteiten is toegestaan zoals bepaald in artikel 1.3.

5.2 Verboden bij elk gebruik (studiegerelateerd of niet) is echter het verzenden van informatie of berichten die het imago, de morele of economische belangen van de UvA kunnen schaden. Voorbeelden hiervan zijn:[4]
- 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 (kunnen) aanzetten tot discriminatie, haat en/of geweld;

[3] Malware is kwaadaardige software die gebruikt wordt om een computersysteem opzettelijk te verstoren. Het doel daarvan varieert van onbruikbaar maken tot het verzamelen van informatie.
[4] Er wordt actie ondernomen op basis van klachten door medewerkers en studenten of andere bronnen (derden). Klachten worden beoordeeld aan de hand van wet- en regelgeving.

- het versturen van berichten aan grote aantallen ontvangers tegelijk, het versturen van kettingbrieven of het verspreiden van kwaadaardige software zoals virussen, wormen, Trojaanse paarden en spyware;

5.3 Het gebruik van computer- en netwerkfaciliteiten ten behoeve van commerciële activiteiten is uitsluitend toegestaan wanneer de UvA hiervoor schriftelijk toestemming heeft verleend.

5.4 Onderdeel van de ICT-faciliteiten die de student ter beschikking gesteld worden zijn filesharing- of streamingdiensten. In het geval dat het gebruik van deze diensten te veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de ICT-faciliteiten in gevaar kan brengen, dan kan de UvA hier tegen optreden.

Artikel 6. Monitoring door de Instelling

6.1 Controle van gebruik van de ICT faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit Reglement voor de doelen genoemd in artikel 1. Verboden gebruik van de faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

6.2 Ten behoeve van deze controle worden geautomatiseerd gegevens verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke ICT beheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld.

6.3 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, doet men zo snel mogelijk melding van de maatregel.

6.4 Bij vermoedens van overtreding van de regels kan 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.

6.5 De UvA 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 UvA de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

Artikel 7. Procedure bij gericht onderzoek

7.1 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.

7.2 Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de decaan van de faculteit, na consultatie van de Functionaris Gegevensbescherming (FG)en goedkeuring van de directeur ICTS welke toestemming de redenen zal noemen waarom deze wordt verleend. Het College van Bestuur en de Functionaris Gegevensbescherming (FG) ontvangen een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

7.3 Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de ICT faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de UvA na aparte toestemming 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.

7.4 Gericht onderzoek naar de beveiliging of integriteit van ICT-faciliteiten mag in afwijking hiervan door ICT beheer 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 het vorige lid worden gevolgd.

7.5 De student wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur 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.

7.6 Geautoriseerde ICTS medewerkers verschaffen zich slechts toegang tot accounts of computers van de student als de student daarvoor zijn toestemming heeft gegeven. Toegang 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.

Artikel 8. Consequenties van overtreding

8.1 Bij het niet opvolgen van instructies of aanwijzingen op basis van dit reglement, bij handelen in strijd met dit reglement of de algemeen geldende wettelijke regels, kan het College van Bestuur afhankelijk van de aard en de ernst van de overtreding disciplinaire 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.

8.2. Er worden geen disciplinaire maatregelen getroffen zonder dat de student gelegenheid heeft gekregen zijn zienswijze naar voren te brengen/

8.3 Behalve een waarschuwing kunnen geen disciplinaire maatregelen worden opgelegd indien de controle slechts heeft plaatsgevonden op basis van een langs geautomatiseerde uitgevoerd verwerking van persoonsgegevens (zoals een constatering op basis van een automatische filter of een blokkade)

8.4 In aanvulling van het voorgaande is het mogelijk dat de UvA 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 ICT beheer is weggenomen. Indien na een week geen verbetering is geconstateerd door ICT beheer, kan ICT beheer besluiten tot een langere blokkade. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

Artikel 9. Slotbepalingen

9.1 In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur.Het CvB wint, afhankelijk van het onderwerp, advies in bij de Chief Security Officer (CSO) en / of de Chief Information Security Officer (CISO) en/of de Functionaris Gegevensbescherming (FG).