Kenmerk	CvB23-0025		
Omschrijving document	**Reglement verantwoord gebruik ICT-faciliteiten studenten**		
College van Bestuur	Definitief vastgesteld	d.d.	12 augustus 2023
Raad van Toezicht	Niet van toepassing		
Ondernemingsraad	Ingestemd		6 juli 2023
Studentenraad	Ingestemd		24 november 2023

mborijnland méér dan mbo

Reglement verantwoord gebruik ICT-faciliteiten door Studenten van mboRijnland

Inleiding

mboRijnland biedt aan de eigen studenten en aan bezoekende studenten de mogelijkheid om diverse ICT-faciliteiten, zoals internetverbindingen, apparatuur en applicaties, te gebruiken. Zo hebben studenten binnen de gebouwen van mboRijnland de mogelijkheid om internet te gebruiken ten behoeve van de studie. Tevens worden aan studenten voor persoonlijk gebruik een instellingsgebonden e-mailbox en digitale leeromgeving en overige faciliteiten beschikbaar gesteld, ten behoeve van de studie.

Aan het gebruik van de faciliteiten zijn regels verbonden, in het kader van de informatieveiligheid, beschikbaarheid, rechten van mboRijnland en eventuele derden en een goede gang van zaken in de gebouwen en op de terreinen van mboRijnland. Deze regels zijn in dit reglement verantwoord gebruik ICT-faciliteiten door studenten opgenomen. Deze regels zijn van toepassing op studenten van mboRijnland en bezoekende 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).

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 te allen tijde veilig zijn en niet overbelast worden, kan mboRijnland het gebruik van de faciliteiten monitoren op de manieren zoals beschreven in 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, 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 mboRijnland is toegestaan, zolang dit gebruik voldoet aan de regels van dit Reglement. Het veranderen van instellingen in apparatuur en toepassingen beschikbaar gesteld door mboRijnland is alleen toegestaan met aparte toestemming van het systeembeheer. Het aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met derden op netwerkaansluitingen is te allen tijde verboden.

Bepaalde faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en een wachtwoord. Deze zijn persoonsgebonden en mogen niet met anderen worden gedeeld. Het systeembeheer kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten. Bij een vermoeden van misbruik van een wachtwoord [of authenticatiemiddel] kan het systeembeheer per direct het betreffende account ontoegankelijk maken.

1.1. Beveiliging door mboRijnland en de student

mboRijnland 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 privacyrechten en schending van intellectuele eigendomsrechten.

Natuurlijk is een perfecte beveiliging onmogelijk. Daarom verwacht mboRijnland 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 te allen tijde 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 mboRijnland, in het kader van beveiliging:

- deze apparatuur te voorzien van een adequate virusscanner en firewall;

- onrechtmatige toegang tot systemen van mboRijnland te voorkomen door moeilijk te raden wachtwoorden en/of pincodes te gebruiken;
- deze apparatuur up-to-date te houden wat betreft software-instellingen.

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 mboRijnland zijn en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van mboRijnland of derden of de integriteit en de veiligheid van het netwerk aantasten.

Onder illegaal, storend en/of overlast veroorzakend gebruik wordt 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 of het verspreiden van kwaadaardige software zoals virussen, wormen, Trojaanse paarden en spyware;
- filesharing- of streamingdiensten (zoals Netflix) of online spellen 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;
- Activiteiten te ondernemen gericht op hacking of andere strafbare activiteiten.

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

1.3.

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

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

Indien mboRijnland 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 mboRijnland

mboRijnland controleert de naleving van dit Reglement. mboRijnland handelt bij de controle op het gebruik van de faciliteiten binnen de geldende wet- en regelgeving.

mboRijnland 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. ,mboRijnland 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 mboRijnland, de bewaking van de integriteit en de

veiligheid van het netwerk, de computerfaciliteiten van mboRijnland. 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, doet de medewerker van IT-operations zo snel mogelijk melding van de maatregel.

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.

mboRijnland 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 mboRijnland 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 mboRijnland 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 mboRijnland 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 (bijvoorbeeld 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. Tevens vindt er op basis van signaleringen op veiligheidsrisico's controle plaats op bestanden die als verdacht zijn aangemerkt. Deze controle wordt slechts gebruikt voor het borgen van de (technische) veiligheid van het netwerk en de systemen van mboRijnland.

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 mboRijnland worden in het kader van de controle op dit Reglement de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij verwerkt worden, juist en nauwkeurig zijn.

Door mboRijnland 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 op verzoek van de directeur van het desbetreffende MBO College en na toestemming van de directeur van het Centrum voor Informatie en Innovatie. Bij deze toestemming dient te worden vastgelegd wat de redenen zijn voor het onderzoek. Het College van Bestuur ontvangt een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek. Tevens kan het College van Bestuur zelfstandig onderzoek laten uitvoeren zonder betrokkenheid van andere directeuren.

Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan mboRijnland 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.

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 het vorige lid worden gevolgd.

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.

Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van de student als de student daarvoor zijn toestemming heeft gegeven. Toegang tot het account van de student zonder deze toestemming is slechts toegestaan in dringende gevallen, waarbij de vertrouwelijkheid, beschikbaarheid of integriteit van de faciliteiten van mboRijnland een risico lopen. Een voorbeeld hiervan is het als er malware wordt verspreid via de account van de student. De systeembeheerder vraagt hiervoor, indien mogelijk, vooraf toestemming aan de teamleider IT operations. De student en de teamleider IT operations zullen 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 mboRijnland, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen.

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

In afwijking van het voorgaande is het mogelijk dat mboRijnland 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 disciplinaire maatregelen worden genomen.

mboRijnland doet te allen tijde aangifte te doen van geconstateerde strafbare feiten.

4. Rechten van de student met betrekking tot persoonsgegevens

De student kan zich tot het bestuur wenden met het verzoek om een volledig overzicht van zijn persoonsgegevens, zoals door mboRijnland verwerkt in het kader van dit Reglement.

De student kan het bestuur verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen, indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn, dan wel het verwerken ervan in strijd met een wettelijk voorschrift is.

De student kan verder bezwaar maken tegen de verwerking van zijn persoonsgegevens, indien er sprake is van bijzondere persoonlijke omstandigheden. In dat geval zal de verwerking gestopt, dan wel beperkt worden, tenzij er sprake is van dwingende gerechtvaardigde belangen, die zwaarder wegen dan de rechten en vrijheden van de student.

De student heeft in sommige gevallen het recht om het verwerken van zijn persoonsgegevens (al dan niet tijdelijk) te beperken. De student kan de verwerking van zijn persoonsgegevens beperken, indien de gegevens mogelijk onjuist zijn, de verwerking onrechtmatig is, de gegevens niet meer nodig zijn, dan wel de student bezwaar tegen de verwerking heeft ingediend.

De student kan het bestuur verzoeken zijn persoonsgegevens te verwijderen indien deze niet meer nodig zijn, hij eerder toestemming heeft gegeven voor het gebruik van zijn gegevens maar deze toestemming nu intrekt, hij bezwaar gemaakt heeft tegen de verwerking, de verwerking onrechtmatig is, dan wel de wettelijk bepaalde bewaartermijn verlopen is.

Op bovengenoemde verzoeken wordt binnen vier weken gereageerd. Deze termijn kan echter met twee maanden worden verlengd om redenen die verband houden me de specifieke privacyrechten of de complexiteit van het verzoek.
Van een dergelijke verlenging van de termijn zal het bestuur de student binnen vier weken op de hoogte stellen. Een weigering is met redenen omkleed. Een toegewezen verzoek zal zo spoedig mogelijk worden uitgevoerd.

5. Slotbepalingen

Dit Reglement kan door het College van Bestuur, na instemming van de studentenraad, worden herzien. Dit reglement vervangt het eerdere reglement op het gebied van reglement verantwoord netwerkgebruik.

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