Stichting Onderwijs
Midden-Limburg

Gebruikersreglement ICT

Leon van Lare RI
Versie 1.1
13 oktober 2021

Dit document voor leerlingen en medewerkers van Stichting Onderwijs Midden-Limburg (SOML) is gebaseerd op Model reglementen voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo, het protocol media en EIC van het Hoeksch Lyceum en op het Aanvaardbaar gebruik van bedrijfsmiddelen van Stichting Kennisnet.

Inhoud

Document geschiedenis

Revisies

Onderstaande tabel beschrijft de geschiedenis van dit document

Versie	Datum	Toelichting
0.3	2-7-2021	Eerste kladopzet
1.1	12-10-2021	Definitieve eerste opzet

Goedkeuring

Dit beleid is goedgekeurd door de onderstaande personen:

Naam	Functie	Versie	Datum
M.J.H.M. Kikken	Voorzitter College van bestuur	1.1	12-10-2021
P.M. Slegers	Lid College van Bestuur	1.1	12-10-2021
Leden van de GMR	GMR	1.1	12-10-2021

0. Samenvatting

Iedereen voldoet aan de algemene normen voor ‘zorgvuldigheid’. Dit zijn (niet uitputtend):

- Het zorgdragen voor goede fysieke en technische bescherming van de EIC (elektronische informatie- en communicatiemiddelen)
- Het voorkomen van het lekken van interne en vertrouwelijke informatie
- Het voorkomen dat beveiligingsmaatregelen worden omzeild door bijvoorbeeld jailbreaks
- Ga zorgvuldig om met persoonlijke gegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht.
- Het onmiddellijk melden van verloren of gestolen bedrijfsmiddelen door het sturen van een e-mail aan de daarvoor aangewezen persoon.
- Voor een datalek (procedure meldplicht datalekken) stuur je een e-mail aan privacy@soml.nl .

1. Inleiding

Voor het goed kunnen uitvoeren van je schoolwerk, is het gebruik van internet en ict-middelen voor alle leerlingen en medewerkers noodzakelijk. De middelen en informatie die hiervoor gebruikt worden noemen we samen de elektronische informatie- en communicatiemiddelen (EIC). De EIC bestaan uit:

- Hardware, bijvoorbeeld je tablet, een schoolcomputer en je telefoon
- Software (of systemen), bijvoorbeeld je SOML e-mail, Microsoft Office of Magister.
- Informatie, bijvoorbeeld e-mails, cijferlijsten en leerlinggegevens
- Internetgebruik, bijvoorbeeld het surfen op internet, het gebruik van web-mail maar ook sociale media.

Bij het gebruik van deze middelen horen risico's die het stellen van gebruiksregels noodzakelijk maken. Hoe jij je werk doet moet veilig zijn en passen binnen wet- en regelgeving. Dit document geeft aan hoe SOML van alle gebruikers (waaronder uitzendkrachten, vrijwilligers, leveranciers en tijdelijk personeel) verwacht dat ze omgaan met de EIC.
De afspraken in dit document gelden voor alle plekken waar je je schoolwerk doet en alle EIC waar je het werk mee doet. De eerste keer dat een gebruiker gebruik maakt van het computernetwerk van SOML wordt beschouwd als het moment van een overeenkomst met SOML met betrekking tot dit document. De leerling / medewerker stemt op dat moment in met de hier genoemde regels en afspraken.

1.1. Uitgangspunten document

Het document stelt regels ten aanzien van het gebruik van de EIC en internet. Het doel van deze regels is het bepalen van de normen en uitgangspunten ten aanzien van:

- Systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
- Tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
- Bescherming van privacy gevoelige informatie waaronder persoonsgegevens van SOML, haar medewerkers, van leerlingen en ouders;
- Bescherming van vertrouwelijke informatie van SOML en haar medewerkers, en van leerlingen en ouders;
- Bescherming van de intellectuele eigendomsrechten van het schoolbestuur en derden. Hierbij horen bijvoorbeeld licentie-afspraken die van toepassing zijn binnen SOML;
- Voorkomen van negatieve publiciteit;
- Kosten- en capaciteitsbeheersing.

De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. SOML 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 EIC en de bescherming van de privacy van leerlingen en medewerkers.

1.2. Eigen verantwoordelijkheid en privégebruik

De ingezette devices (inclusief eigen devices, ook wel ‘Own Device’ genoemd) blijven jóuw verantwoordelijkheid. Je dient zorgvuldig om te gaan met door de school beschikbaar gestelde EIC. Ook als je bijvoorbeeld je laptop uitleent aan iemand anders of wanneer jij je eigen tablet, die je voor school gebruikt, uitleent aan een familielid.
Wanneer er toch anderen van het apparaat gebruik maken zorg je ervoor dat je de toegang tot leermiddelen van SOML beperkt door in ieder geval:

- Het blokkeren van toegang tot school e-mail en informatie door middel van een wachtwoord
- Persoonlijk toezicht te houden op het gebruik

Je account en wachtwoord zijn strikt persoonlijk en deel je nooit met iemand anders.
Leerlingen mogen slechts gebruik maken van hun mobiele telefoons, smartphone’s, smartwatches of vergelijkbare EIC op tijden, plaatsen en op de wijze die de schoolleiding heeft bepaald. De schoolleiding heeft de bevoegdheid het gebruik van deze middelen geheel te verbieden.
Van medewerkers van SOML en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bijvoorbeeld personeelsdossiers, vertrouwelijke enquêtegegevens, zorgdossiers et cetera 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. Afspraken

2.1. Computergebruik

Computer- en netwerkfaciliteiten worden voor je schoolwerk beschikbaar gesteld. Bij het gebruik van ICT-middelen is gaan we uit van de volgende afspraken:

- Bij het tijdelijk verlaten van de werkplek vergrendel je je desktop (bij Windows bijvoorbeeld via windowstoets-L)
- Sla (persoons)gegevens alleen op de daarvoor aangewezen devices op. Deze systemen worden regelmatig via een geautomatiseerd proces gescand op de fysieke aanwezigheid van programma’s (.exe, .com bestanden) en inhoudelijk op de aanwezigheid van bestanden met pornografische, racistische, discriminerende, gewelddadige of anderszins onacceptabele, dan wel niet voor het onderwijs aan SOML bestemde inhoud. De beoordeling hiervan ligt in handen van de schoolleiding.
- Het is niet toegestaan bestanden van bovengenoemde aard te downloaden, op het netwerk te plaatsen, in bezit te hebben of van deze bestanden gebruik te maken. Dit geldt ook voor het gebruik van deze bestanden via externe drives (zoals bijvoorbeeld een USB stick).
- Meld storingen bij afdeling ICT van je school.

2.2. Minimale beveiligingsmaatregelen voor eigen devices

Bij het gebruik van eigen devices (de 'Own Devices' zoals laptop, smartphone of tablet) op school dienen er een aantal beveiligingsmaatregelen genomen te worden. Als je een device van de school gebruikt, dan mag je ervan uit gaan dat SOML deze maatregelen geregeld heeft. Voor alle EIC moeten minimaal de volgende beveiligingsmaatregelen genomen zijn:

- Bescherm de toegang met een wachtwoord of, in het geval van een tablet of smartphone, met een pincode of vingerafdruk.
- Zorg dat je device vergrendeld is wanneer je er niet bij in de buurt bent, zodat niemand bij jouw bestanden en gegevens kan.
- Wanneer het apparaat weer in gebruik genomen wordt moet het om een wachtwoord, pincode of vingerafdruk vragen.
- Je dient software up-to-date te houden door periodieke updates (minimaal maandelijks).
- Je dient goede maatregelen tegen virussen of malware te hebben genomen. Bijvoorbeeld door periodiek (minimaal maandelijks) of continu je device te scannen.
- Voor medewerkers geldt: alle gegevens van SOML dienen versleuteld te zijn als deze, om welke reden dan ook, tijdelijk niet op het schoolnetwerk opgeslagen worden (denk hierbij aan het eigen device of USB stick).

SOML mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van SOML moet je zelf aantonen dat de bovenstaande maatregelen worden toegepast.

2.3. Gebruik van e-mail

Het e-mailsysteem en de bijbehorende mailbox worden voor het uitoefenen van je schoolwerk beschikbaar gesteld. Gebruik hiervan is verbonden aan school werkzaamheden en gaan uit van de volgende afspraken:

- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.
- Gebruik het school e-mail adres alléén voor school gerelateerde zaken.
- Gebruik voor privé e-mail een eigen privé e-mailadres via een externe webmaildienst.

2.4. Gebruik van het schoolnetwerk

Bij het gebruik van het schoolnetwerk en de bijbehorende faciliteiten gaan we uit van de volgende afspraken:

- Het schoolnetwerk is alleen toegankelijk voor geregistreerde gebruikers.
- De gebruikersnaam en het bijbehorend wachtwoord zijn strikt persoonlijk en mogen niet aan anderen worden doorgegeven. Ditzelfde is van toepassing op alle door de school verstrekte inloggegevens (o.a. Magister, wifi, public cloud).
- Iedereen dient bij (vermoeden van) misbruik van diens gegevens of bij (vermoeden van) inbreuken op de beveiliging van het schoolnetwerk, van binnenuit of van buiten de school, contact op te nemen met afdeling ICT.
- Het is niet toegestaan om zich moedwillig toegang te verschaffen tot andermans gegevens of bestanden.

- Onbedoelde inbreuk op beveiliging, van binnenuit of van buiten de school dient onmiddellijk aan de schoolleiding gemeld te worden.

2.5. Gebruik van internet en sociale media

Bij het gebruik van internet en de bijbehorende faciliteiten gaan we uit van de volgende afspraken:

- Beperkt persoonlijk gebruik is toegestaan, mits dit
  - niet storend is voor de dagelijkse werkzaamheden
  - niet voor commerciële doeleinden is en
  - geen verboden gebruik oplevert.
- Het is niet toegestaan om op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten.
- Het is niet toegestaan films, muziek, software en overig auteursrechtelijk beschermd materiaal zonder toestemming te downloaden.
- Het deelnemen aan kansspelen is niet toegestaan.
- Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale netwerken en andere vergelijkbare communicatienetwerken over alle aan school verbonden gebruikers. Dit geldt in het bijzonder ook voor internetgebruik buiten het schoolnetwerk met betrekking tot aan de school verbonden gebruikers/personen.
- Er wordt van iedereen verwacht dat zij:
  - het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken) en websites
  - bij het verwerken van persoonsgegevens alléén gebruik maken van bekende én beveiligde draadloze netwerken
  - weten wat malware en phishing is, het kunnen herkennen en weten hoe te handelen
- Bij SOML gelden verder de volgende afspraken voor het gebruik van sociale media:
  - Deel op verantwoorde wijze kennis via sociale media rekening houdend met de goede naam van SOML en iedereen die hierbij betrokken is.
  - Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens SOML gedaan wordt.
  - Publiceer geen vertrouwelijke informatie op sociale media.
  - Publiceer geen beeld- of geluidsmateriaal van personen zonder de uitdrukkelijke voorafgaande aantoonbare toestemming. Bij leerlingen is toestemming nodig van ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder is dan 16 jaar.
  - Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn. Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren. Neem contact op met een leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met SOML.

2.6. Wachtwoorden en pincodes

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.

- Wachtwoorden moeten voldoen aan het wachtwoordbeleid van SOML. Dat verschilt voor medewerkers en leerlingen. Voor leerlingen moet het wachtwoord voldoen aan woordenboek-complexiteit. Bij medewerkers geldt de Microsoft-security-policy met gemiddelde complexiteit.
- Pincodes moeten minstens 4 tekens zijn.

3. Controle EIC

SOML handelt binnen de geldende wet- en regelgeving, te weten:
De Grondwet, algemene Verordening Gegevensbescherming (AVG), Wet Medezeggenschap Onderwijs (WMO), Burgerlijk Wetboek (BW), Wetboek van Strafrecht, Cao VO.
SOML zal bij controle van het gebruik van EIC uitgaan van de juiste balans tussen verantwoord gebruik en bescherming van de privacy van leerlingen.

3.1. Controle

Voor controle op naleving van dit reglement gelden de volgende voorwaarden en afspraken:

- Controle van persoonsgegevens over e-mail- en internetgebruik vindt slechts plaats in het kader van handhaving van de doelen uit dit reglement.
- Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
- Al het computergebruik wordt automatisch vastgelegd, waaronder aanmelding op het netwerk, gebruikte applicaties, bezochte website, et cetera.
- Niet toegestaan gebruik van elektronische informatie- en communicatiemiddelen wordt zoveel mogelijk technisch onmogelijk gemaakt.
- De gebruiker is zich bewust van het feit dat alle computerhandelingen van hem of haar kunnen worden vastgelegd in digitale logboeken.
- Om de veiligheid van het netwerk te waarborgen en toe te zien op een zorgvuldig gebruik, worden van tijd tot tijd controles uitgevoerd. Deze controles bestaan onder andere uit het periodiek scannen van de persoonlijke schijfruimte.
- Opdrachten van leerlingen kunnen door middel van een gespecialiseerd programma worden gecontroleerd op plagiaat.

4. Sancties

Bij handelen in strijd met dit reglement of de algemeen geldende wettelijke regels, kan het bestuur afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, account-blokkering, schadevergoeding, schorsing en aangifte bij de politie. Een account-blokkering kan direct in werking worden gesteld. Maar voordat tot het treffen van een disciplinaire maatregel zal worden overgegaan, vindt altijd hoor en wederhoor plaats.

5. Slotbepaling

De GMR is toestemmingsgerechtigd voor dit gebruikersreglement. Deze regeling wordt eens per 2 jaar geëvalueerd door SOML en de GMR. De organisatie kan dit reglement met instemming van de GMR wijzigen als de omstandigheden daar aanleiding toe geven.