Reglement ICT middelen

leerlingen

CMT: 9 maart 2021

MR: 1 juli 2021

CvB: 2 juli 2021

Assen, 8 december 2020
Bestuurssecretariaat
Judith Bordewijk

Inhoud

Dit document voor leerlingen van Dr. Nassau College 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.

1. Inleiding

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

- Hardware, bijvoorbeeld een tablet, een schoolcomputer en een telefoon
- Software (of systemen), bijvoorbeeld het school e-mail-account en Microsoft Office
- Informatie, bijvoorbeeld e-mails, cijferlijsten en leerlinggegevens.

Daar waar in dit document wordt gesproken over devices wordt EIC bedoeld.

Aan het gebruik van deze middelen zijn risico's verbonden die het stellen van gedragsregels noodzakelijk maken. Hoe leerlingen hun schoolwerk doen moet veilig zijn en passen binnen wet- en regelgeving. Dit document beschrijft de verwachtingen die het Dr. Nassau College van leerlingen heeft in de omgang met devices. De afspraken in dit document gelden voor alle plekken waar leerlingen hun schoolwerk doen en alle devices waar leerlingen mee werken. De eerste keer dat leerlingen gebruik maken van het computernetwerk van het Dr. Nassau College wordt beschouwd als de totstandkoming van een overeenkomst tussen het Dr. Nassau College en de leerlingen met betrekking tot dit document, waarbij de leerlingen instemmen met de in dit document verwoorde regels en afspraken.

1.1. Uitgangspunten document

Het document stelt regels ten aanzien van het gebruik van de devices en internet door leerlingen. 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 het schoolbestuur en haar medewerkers en van leerlingen en ouders;
- Bescherming van vertrouwelijke informatie van het schoolbestuur en haar medewerkers en van leerlingen en ouders;
- Bescherming van de intellectuele eigendomsrechten van het schoolbestuur en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen het schoolbestuur;
- Voorkomen van negatieve publiciteit;
- Kosten- en capaciteitsbeheersing.

1.2. Eigen verantwoordelijkheid en privégebruik

Leerlingen zijn verantwoordelijk voor de schoolmiddelen die aan hen zijn toevertrouwd. Zij dienen zorgvuldig om te gaan met door de school beschikbaar gestelde pc's en andere informatie- en communicatiemiddelen. Wanneer anderen van het apparaat gebruik maken zorgen leerlingen ervoor dat de toegang tot leermiddelen van het Dr. Nassau College is beperkt door bijvoorbeeld:

- Het blokkeren van toegang tot school e-mail en informatie door middel van een wachtwoord
- Het aanmaken van een apart user account voor andere gebruikers

- Continu persoonlijk toezicht te houden op het gebruik

Het account en wachtwoord zijn strikt persoonlijk en worden nooit met iemand anders gedeeld. Leerlingen mogen slechts gebruik maken van hun mobiele telefoons, smartphone's, smartwatches, tablets of vergelijkbare informatie- en communicatiemiddelen 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. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen zoals het ontzeggen van toegang van een informatie- of communicatiemiddel.

2. Afspraken

In dit hoofdstuk staat een aantal afspraken genoemd waar leerlingen zich aan dienen te houden.

2.1. Algemene normen

Leerlingen voldoen aan de algemene normen voor 'zorgvuldigheid'. Dit zijn (niet uitputtend):

- Het zorgdragen voor goede fysieke bescherming van devices.
- Het zorgdragen voor goede technische bescherming van devices (zie 2.3).
- Het voorkomen van het lekken van interne en vertrouwelijke informatie.
- Het voorkomen dat beveiligingsmaatregelen worden omzeild door bijvoorbeeld jailbreaks.
- Het onmiddellijk na constatering melden van verloren of gestolen communicatiemiddelen waarop informatie van de school staan door te bellen naar 0592 – 333 107

2.2. Computergebruik

Computer- en netwerkfaciliteiten worden voor het uitoefenen van hun werkzaamheden aan leerlingen beschikbaar gesteld. Gebruik van ict-faciliteiten is verbonden aan deze werkzaamheden en gaan uit van de volgende afspraken:

- Het installeren van software op de computer van het Dr. Nassau College is niet toegestaan zonder toestemming en eventuele benodigde licenties.
- Wachtwoorden zijn persoonlijk en worden niet gedeeld, ook niet incidenteel.
- Leerlingen sluiten na gebruik de computer af of loggen uit.
- Bij het tijdelijk verlaten van de werkplek vergrendelen leerlingen de pc (windowstoets-L)
- Leerlingen hebben de beschikking over eigen schijfruimte in het netwerk om hun gegevens op te slaan.
- Deze ruimte wordt regelmatig door het systeembeheer gescand op de fysieke aanwezigheid van programma's (.exe, .com) en inhoudelijk op de aanwezigheid van bestanden met pornografische, racistische, discriminerende, gewelddadige of anderszins onacceptabele, dan wel niet voor het onderwijs aan het Dr. Nassau College 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 opstarten van deze bestanden via externe drives.

- Externe datadragers, zoals USB-sticks, zijn niet toegestaan.
- In gevallen waar vanwege de overheid en/of school het gebruik van een USB-stick wordt voorgeschreven, kan deze worden gebruikt met inachtneming van de voorgeschreven voorzorgsmaatregelen.

2.3. Minimale beveiligingsmaatregelen voor eigen devices

Bij het gebruik van eigen devices (laptop, tablet of iPad) op school dient een aantal beveiligingsmaatregelen genomen te worden. Als leerlingen een device van de school gebruiken, dan mogen zij ervan uitgaan dat het Dr. Nassau College deze maatregelen hierop geregeld heeft.
Voor alle devices moeten minimaal de volgende beveiligingsmaatregelen genomen zijn:

- De toegang is beschermd met een wachtwoord of, in het geval van een iPad of tablet, met een pincode.
- Het device is vergrendeld wanneer leerlingen niet bij in de buurt zijn zodat niemand bij de bestanden en gegevens kan (windowstoets-L).
- Wanneer het apparaat weer in gebruik genomen wordt moet het om een wachtwoord of pincode vragen.
- Software wordt up-to-date gehouden door periodieke updates (minimaal maandelijks).
- Er zijn goede maatregelen tegen virussen of malware genomen. Bijvoorbeeld door periodiek (minimaal maandelijks) de laptop te scannen.

Het Dr. Nassau College mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van het Dr. Nassau College moeten leerlingen zelf aantonen dat de bovenstaande maatregelen worden toegepast.

2.4. Gebruik van e-mail

Het e-mailsysteem en de bijbehorende mailbox worden aan leerlingen voor het uitoefenen van de studiewerkzaamheden op school beschikbaar gesteld. Bij gebruik van e-mailfaciliteiten van de school gelden de volgende afspraken:

- Leerlingen gebruiken voor school gerelateerde communicatie het e-mail systeem van het Dr. Nassau College.
- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.
- E-mail mag niet gebruikt worden voor ‘verboden handelingen’ (zie 2.9).

2.5. Gebruik van schoolnetwerk

Het gebruik van het schoolnetwerk en de bijbehorende faciliteiten worden aan leerlingen voor het uitoefenen van hun studiewerkzaamheden op school beschikbaar gesteld. Gebruik hiervan is verbonden aan deze werkzaamheden en gaan uit van de volgende afspraken:

- Het schoolnetwerk is alleen toegankelijk voor geregistreerde gebruikers.

- Leerlingen mogen alleen met hun eigen account gebruik maken van het leerling netwerk. Na gebruik sluiten leerlingen hun eigen account ook weer af.
- 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.
- Leerlingen dienen bij (vermoeden van) misbruik van hun gegevens of bij (vermoeden van) inbreuken op de beveiliging van het schoolnetwerk, van binnenuit of van buiten de school, direct contact op te nemen met de ICT-medewerker op de locatie.
- Het is leerlingen 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.

2.6. Gebruik van internet

Het gebruik van internet en de bijbehorende faciliteiten worden aan leerlingen voor het uitoefenen van hun studiewerkzaamheden op school beschikbaar gesteld. Gebruik hiervan is verbonden aan deze werkzaamheden en gaan uit van de volgende afspraken:

- Internet wordt gebruikt voor schooldoeleinden.
- Het is niet toegestaan om op websites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten.
- Het is niet toegestaan om films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron.
- Het is niet toegestaan om spelletjes te spelen en gamewebsites te bezoeken, anders dan in opdracht van en met toestemming van de docent of de beheerder.
- 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.
- Het is niet toegestaan om je actief te onttrekken aan de beveiligde omgeving van de school (bijvoorbeeld door gebruik te maken van hotspots of een VPN dienst).

2.7. Gebruik beeld- en geluidsmateriaal

Voor het gebruiken, maken en delen van beeld- en geluidsmateriaal, het delen van foto's en video's van leerlingen en/of medewerkers hanteren wij de volgende regels:

- Het is niet toegestaan om film, video-, en/of geluidsopnamen of ander materiaal van medeleerlingen, op school werkzame personen en of andere bij de school betrokken personen te maken en/of via (elektronische) informatie- en communicatiemiddelen openbaar te maken, tenzij medewerkers van het Dr. Nassau College uitdrukkelijk toestemming hebben gegeven voor plaatsing.

- Voor het maken en/of openbaar maken van beeld en/of geluidsopnamen waarop personen herkenbaar, zichtbaar of hoorbaar zijn, is voorafgaande toestemming van betrokkene(n) of diens wettelijke vertegenwoordiger(s) vereist.

Voor de afspraken rondom het delen van beeld- en geluidsmaterialen via social media verwijzen we naar het ‘social media protocol’ van het Dr. Nassau College.

2.8. 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 minimaal 8 tekens bevatten, met minstens drie van de volgende vier elementen :
  1) kleine letters
  2) hoofdletters,
  3) cijfers,
  4) speciale karakters (!@#$%^&*().
- Pincodes moeten langer dan 4 tekens zijn.
- Wachtwoorden moeten volgens de afspraken binnen het Dr. Nassau College op aangegeven tijden vervangen worden.
- Gebruik niet voor elke systeem hetzelfde wachtwoord
- *Wachtwoorden zijn persoonlijk en mogen niet gedeeld worden, ook niet incidenteel!*

2.9. Verboden handelingen

Het is niet toegestaan om bij wet verboden handelingen uit te voeren op een device wat voor Dr. Nassau College werkzaamheden gebruikt wordt. Dit zijn (niet uitputtend):

- Het opslaan of delen van illegale en/of aanstootgevende bestanden
- Criminele activiteiten
- Het gebruik van illegale software en/of het omzeilen van licenties
- Alle handelingen die de veiligheid van het netwerk van het Dr. Nassau College kunnen schaden zoals hotspots en VPN.

3. Controle devices

Het Dr. Nassau College 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. Het Dr. Nassau College zal bij controle van het gebruik van devices vanuit dit reglement 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 websites etc.
- Niet toegestaan gebruik van elektronische informatie- en communicatiemiddelen wordt zoveel mogelijk technisch onmogelijk gemaakt.
- Door middel van 'meekijksoftware' is het mogelijk dat personeel van Dr. Nassau College meekijkt met leerlingen.
- Leerlingen zijn 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 op verboden bestanden; zie 2.9.
- Opdrachten van leerlingen kunnen door middel van een gespecialiseerd programma worden gecontroleerd op plagiaat.

4. Sancties

Bij handelen in strijd met deze gedragscode 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.

Leerlingen die zich niet aan deze gedragscode houden, worden zo spoedig mogelijk op hun gedrag aangesproken. Ouders worden ook ingelicht. Zij krijgen daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. De school en leerlingen maken dan afspraken voor de toekomst en bepalen de mogelijke sanctie(s) bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in deze gedragscode bepaalde. Ook kan de toegang tot e-mail of internet worden beperkt of geheel worden afgesloten. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens worden getroffen, zoals een constatering van een automatisch filter of blokkade. Verder worden geen disciplinaire maatregelen getroffen zonder dat leerlingen gelegenheid hebben gekregen hun zienswijze naar voren te brengen.

5. Slotbepaling

Deze regeling wordt jaarlijks geëvalueerd.