

Gedragscode voor ict- en internetgebruik voor leerlingen

Versie 1.1 - 13 november 2023 (Gepasseerd bij de GMR op 13 december 2023)

Bron: Kennisnet Informatiebescherming en Privacy

Dit document voor leerlingen is gebaseerd op Modelreglementen voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo, het protocol media en EIC van het Hoeksch Lyceum, het Protocol sociale media van het Clusius College en op het Aanvaardbaar gebruik van bedrijfsmiddelen van Stichting Kennisnet.

Inhoud

0. Document geschiedenis	2
0.1 Revisies	2
0.2 Goedkeuring	2
1. Inleiding	3
1.1 Uitgangspunten gedragscode ict- en internetgebruik.....	3
1.2 Eigen verantwoordelijkheid en privégebruik	3
2. Gedragsregels	4
2.1 Algemene normen.....	4
2.2 Wachtwoorden en pincodes	4
2.3 Gebruik van ict-middelen (hardware) beschikbaar gesteld door school	5
2.4 Minimale beveiligingsmaatregelen voor eigen apparaten	5
2.5 Gebruik van e-mail.....	6
2.6 Gebruik van de digitale leeromgeving	6
2.7 Gebruik van internet/wifi op school.....	6
2.8 Gebruik beeld- en geluidsmateriaal.....	7
2.9 Online onderwijs	7
2.10 Sociale media	8
2.11 Verboden handelingen	9
3. Controle internet en ict-gebruik.....	10
3.1 Controle op naleving gedragsregels.....	10
3.2 Controle op plagiaat.....	11
4. Sancties	11
5. Slotbepaling.....	11

0. Document geschiedenis

0.1 Revisies

Onderstaande tabel beschrijft de geschiedenis van dit document

Versie	Datum	Toelichting
1.1	13 nov 2023	Invoering modelreglement van Kennisnet Informatiebescherming en Privacy (IBP). Vervangt social media reglement. Voor review directies, GMR en leerlingenraad.

0.2 Goedkeuring

Dit beleid is goedgekeurd door de onderstaande personen:

Naam	Functie	Versie	Datum
D. Roobeek	Directeur-bestuurder	1.1	13 nov 2023

1. Inleiding

Om het onderwijs goed te kunnen volgen gebruiken leerlingen internet en ict-middelen. Bij ict-middelen kan je denken aan:

- Hardware, apparaten zoals je tablet, een laptop, een schoolcomputer en je mobiele telefoon
- Software (of systemen), bijvoorbeeld je email-account van school en je digitale rooster
- Informatie, bijvoorbeeld e-mails, cijferlijsten en leerling- en docentgegevens

Internet en ict-middelen hebben veel voordelen voor leerlingen, zo kunnen ze snel hun rooster controleren op hun telefoon en opdrachten digitaal inleveren. Maar, er kleven ook risico's aan het gebruik ervan. Naast de afleidingen van social media kan een foto of bericht die een leerling deelt met een Whatsapp-groep bijvoorbeeld zonder dat de leerling het wil door anderen doorgestuurd worden, hackers kunnen de ict-systemen in je school platleggen. Het is dus belangrijk dat ook leerlingen bij het gebruik van internet en ict-middelen voor school veilig werken, rekening houden met anderen en zich houden aan de gedragsregels en de wet.

Deze gedragscode ict- en internetgebruik geeft aan hoe onze school van leerlingen verwacht dat ze omgaan met internet en ict-middelen. De regels die zijn beschreven in de gedragscode gelden voor alle plekken waar een leerling schoolwerk doet en alle ict-middelen waarmee de leerling dit doet.

1.1 Uitgangspunten gedragscode ict- en internetgebruik

In de gedragscode zijn de regels beschreven die gelden als leerlingen gebruik maken van internet en ict-middelen voor hun schoolwerk en andere zaken die verband houden met school. Met deze regels wil de school de volgende doelen bereiken:

- Zorgen voor een veilige digitale schoolomgeving, inclusief beveiliging tegen schade en misbruik
- Tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten
- Bescherming van privacygevoelige 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
- Zorgen dat het ict- en internetgebruik betaalbaar blijft voor de school en dat er genoeg ruimte op de systemen en de verbinding (capaciteit) is zodat alle leerlingen en medewerkers hun werk kunnen doen

1.2 Eigen verantwoordelijkheid en privégebruik

Een leerling is zelf verantwoordelijk voor de ict-middelen die de school ter beschikking stelt. De leerling gaat zorgvuldig om met door de school beschikbaar gestelde pc's, laptops en andere ict-middelen. Ook als een leerling bijvoorbeeld zijn of haar schoollaptop uitleent

aan een andere leerling of wanneer een leerling een eigen tablet, die hij of zij voor school gebruikt, uitleent aan een familielid.

Wanneer een leerling iemand anders zijn of haar eigen apparaat laat gebruiken zorgt de leerling ervoor dat diegene geen toegang heeft tot de applicaties en leermiddelen van school 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 bijvoorbeeld broertjes, zusjes of ouders
- Continu persoonlijk toezicht te houden op het gebruik

Het schoolaccount en wachtwoord van een leerling zijn strikt persoonlijk. De leerling deelt dit nooit met iemand anders.

Leerlingen mogen hun mobiele telefoons, smartwatches, tablets of vergelijkbare apparaten alleen gebruiken 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.

2. Gedragsregels

2.1 Algemene normen

Iedere leerling gaat zorgvuldig om met het internet en de ict-middelen van school. Dit betekent in ieder geval dat:

- je netjes omgaat met vertrouwelijke informatie over anderen
- je beveiligingsmaatregelen van de school niet omzeilt of probeert te omzeilen
- je het direct meldt als een apparaat dat de school aan jou ter beschikking heeft gesteld is verloren of gestolen. Je meldt dit bij de conciërge of ICT.

2.2 Wachtwoorden en pincodes

Het beveiligen van toegang tot je schoolaccount, het netwerk, (online) applicaties en apparaten (pc, laptop, telefoon) begint met een goed wachtwoord. Een lang wachtwoord of een 'wachtzin' is beter dan een kort complex wachtwoord.

- Wachtwoorden moeten minimaal 12 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 school op aangegeven tijden vervangen worden.
- Gebruik het wachtwoord alleen voor het schoolaccount en niet voor accounts van andere apps en games.
- Gebruik niet voor elk systeem hetzelfde wachtwoord.

- *Wachtwoorden zijn persoonlijk en mogen niet gedeeld worden, ook niet incidenteel!*

2.3 Gebruik van ict-middelen (hardware) beschikbaar gesteld door school

De school stelt apparaten (hardware, zoals computers, laptops, tablets) beschikbaar zodat leerlingen onderwijs kunnen volgen en hun schoolwerk kunnen doen. Als je hiervan gebruik maakt gelden de volgende regels:

- De apparaten op school zijn bedoeld voor schoolwerk, niet voor privé zaken.
- Het installeren van eigen applicaties/software op apparaten van de school is niet toegestaan zonder toestemming van de ICT-afdeling en eventuele benodigde licenties.
- Je sluit na gebruik op school het apparaat af of logt uit.
- Bij het tijdelijk verlaten van de werkplek vergrendel je het apparaat (windowstoets-L)
- Iedere leerling heeft de beschikking over eigen schijfruimte op services van school om zijn of haar bestanden gegevens op te slaan.
- Deze ruimte wordt door het systeembeheer gescand op de aanwezigheid van illegale software/applicaties en inhoudelijk op de aanwezigheid van bestanden met pornografische, racistische, discriminerende, gewelddadige of anderszins onacceptabele inhoud. De schoolleiding beoordeelt dit.
- Het is niet toegestaan bestanden van bovengenoemde aard op apparaten van school te downloaden, op het netwerk van school 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 (bijvoorbeeld USB stick).

2.4 Minimale beveiligingsmaatregelen voor eigen apparaten

Bij het gebruik van eigen apparaten (laptop, tablet of iPad) op school zorg je voor een aantal beveiligingsmaatregelen. Als je een apparaat van de school gebruikt, dan mag je ervan uit gaan dat de school deze maatregelen hierop getroffen heeft.

Voor alle eigen apparaten moeten minimaal de volgende beveiligingsmaatregelen genomen zijn:

- Bescherm de toegang met een wachtwoord een pincode of andere toegangscode (bijv. vingerafdruk).
- Zorg dat je apparaat vergrendeld is wanneer je er niet bij in de buurt bent, zodat niemand bij jouw bestanden en gegevens kan (windowstoets + L).
- Wanneer het apparaat weer in gebruik genomen wordt moet het om een wachtwoord of pincode of andere toegangscode vragen.
- Je houdt de software up-to-date te door periodieke updates (minimaal maandelijks).
- Je neemt goede maatregelen tegen virussen of malware. Bijvoorbeeld door een virusscanner te installeren en regelmatig je apparaat te scannen. Op een Windowscomputer zit al een gratis virusscanner en je hebt geen betaalde versie nodig.

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

2.5 Gebruik van e-mail

Het e-mailsysteem en de bijbehorende mailbox worden aan de leerling beschikbaar gesteld voor het volgen van onderwijs en het doen van schoolwerk. Daarbij gelden de volgende regels:

- De school, medewerkers/docenten, sturen schoolgerelateerde e-mails altijd naar het e-mailaccount dat je van school hebt gekregen. Het is je eigen verantwoordelijkheid om de schoolmailbox regelmatig te controleren.
- Als je zelf een schoolgerelateerde e-mail wilt sturen, gebruik je daarvoor het e-mailaccount dat je van school hebt gekregen.
- Als je een privémail wilt versturen gebruik je daarvoor niet je schoolaccount, maar een externe webmaildienst. Privégebruik van het school e-mailadres is incidenteel toegestaan.
- E-mail mag niet gebruikt worden voor 'verboden handelingen'; zie 2.11.

2.6 Gebruik van de digitale leeromgeving

Het gebruik van de digitale leeromgeving wordt voor het volgen van onderwijs en het maken van schoolwerk aan de leerling beschikbaar gesteld. Daarbij gelden de volgende regels:

- Het schoolnetwerk is alleen toegankelijk met je schoolaccount.
- De gebruikersnaam en het bijbehorend wachtwoord zijn strikt persoonlijk en mag je niet door anderen laten gebruiken. Dit geldt voor alle door de school verstrekte inloggegevens voor schoolsystemen en -applicaties.
- Voor apps en games die niet voor schoolwerk zijn, maar privé, gebruik je niet je schoolaccount, maar een privé-account.
- Je mag ook geen gebruik maken van de inloggegevens of inbreken in het schoolaccount van andere leerlingen of medewerkers.
- Als je weet of vermoedt dat er misbruik van jouw inloggegevens is gemaakt of als je weet of vermoedt dat anderen, van binnen of van buiten de school, de beveiliging van de digitale leeromgeving proberen te omzeilen dan neem je direct contact op met de afdeling ICT of privacy@jouwschool.nl.
- Mocht je er bij toeval achterkomen dat het mogelijk is om de beveiliging van de digitale leeromgeving te omzeilen, dan meld je dat onmiddellijk aan ICT of privacy@jouwschool.nl.

2.7 Gebruik van internet/wifi op school

Voor het volgen van onderwijs en het maken van schoolwerk op school stelt de school het gebruik van internet en de bijbehorende faciliteiten aan de leerlingen ter beschikking. Daarbij gelden de volgende regels:

- Internet wordt gebruikt voor schooldoeleinden.
- Het is niet toegestaan om internetsites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten.
- Het is niet toegestaan films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron en/of als het downloaden ervan het internet van school overbelast.
- Het is niet toegestaan om spelletjes te spelen en gamewebsites te bezoeken, anders dan in opdracht van en met toestemming van de docent.

- Het bezoeken van chatboxen of vergelijkbare toepassingen is alleen toegestaan in het kader van lesopdrachten.
- Het deelnemen aan gokspelletjes (kansspelen) is niet toegestaan.
- Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale media en andere vergelijkbare communicatienetwerken over alle aan school verbonden gebruikers. Dit geldt in het bijzonder ook voor internet- en sociale media-gebruik buiten het schoolnetwerk als het gaat om aan de school verbonden personen, zoals medeleerlingen, leraren en andere schoolmedewerkers.

2.8 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 andere bij de school betrokken personen te maken en/of via (elektronische) informatie- en communicatiemiddelen openbaar te maken, tenzij de directie van school uitdrukkelijk toestemming heeft gegeven voor plaatsing.
- Voor het maken en/of openbaar maken van beeld en/of geluidsopnamen waarop personen herkenbaar, zichtbaar of hoorbaar zijn, is (daarnaast) voorafgaande toestemming van betrokkene(n) of diens wettelijke vertegenwoordiger(s) vereist.

Voor verdere afspraken rondom het delen van beeld- en geluidsmaterialen via social media verwijzen we naar het *Reglement internet en sociale media op school voor leerlingen*.

2.9 Online onderwijs

Alle regels in deze gedragscode gelden ook als onderwijs (deels) online gegeven wordt. Dit geldt met name – maar zeker niet alleen – voor de volgende regels:

- Je neemt alleen deel aan online lessen waarvoor je bent uitgenodigd en bent gedurende de gehele les aanwezig.
- Je deelt de link van de online les niet met anderen die niet voor de les zijn uitgenodigd.
- Andere personen, zoals ouders, broers en zussen of andere huisgenoten, kijken en luisteren niet mee met jouw online lessen.
- Het is niet toegestaan om foto's, schermafbeeldingen, video's en/of geluid van de online lessen op te nemen, op te slaan, bewerken en/of delen op sociale media. Dat geldt ook voor andere personen, zoals ouders/verzorgers/huisgenoten.
- De rechten op het beeldmateriaal van online lessen liggen bij de school.
- Als je iets niet zou doen in *real life*, doe het dan ook niet online. De reguliere regels van school gelden ook online: bijvoorbeeld het anti-pestprotocol.

Als je weet of vermoedt dat deze regels worden overtreden, neem dan contact op met je mentor, afdelingsleider of directeur.

2.10 Sociale media

Sociale media is de verzamelnaam voor alle toepassingen op het internet waarmee het mogelijk is om met elkaar te communiceren en informatie te delen.

Voor het gebruik van social media door leerlingen gelden de volgende regels:

1. Je bent zelf verantwoordelijk voor alles wat je schrijft of plaatst op het internet. Plaats berichten alleen onder je eigen naam, verspreid geen berichten uit naam van de school. Als leerling ben je ambassadeur van de school. Plaats dan ook nooit berichten die het imago van de school en/of de medewerkers of medeleerlingen kunnen schaden. Bij twijfel geldt in dit geval: Niet plaatsen.
2. Iedereen is verantwoordelijk voor wat hij/zij zelf plaatst op sociale media, en kan daarop aangesproken worden. Ook het doorsturen (forwarden) en herplaatsen (retweeten) zijn handelingen waar je op aangesproken kunt worden. Voor sociale media gelden dezelfde regels die gelden voor pesten. Zie daarvoor ons anti-pestprotocol.
3. Bijdragen op sociale media blijven altijd vindbaar en zoekmachines onthouden alle berichten. Soms ook berichten die verwijderd zijn. Wees je daarvan bewust.
4. Zorg dat je weet hoe de sociale media werken voordat je ze gebruikt, zorg dat de instellingen goed staan en je niet meer informatie deelt dan je wilt. Alles wat wordt gecommuniceerd via internet en sociale media blijft nog lang vindbaar. Bij het gebruik van internet en sociale media houden we rekening met de goede naam van de scholen van CVO 't Gooi en iedereen die daarbij betrokken is zoals docenten, onderwijsondersteunend personeel en ouders.
5. We helpen elkaar om goed en verstandig met sociale media om te gaan en we spreken elkaar daarop aan. Als dat niet lukt, dan vragen we daarvoor hulp aan onze mentor, afdelingsleider of rector.
6. De docent moet vooraf toestemming geven om een mobiele telefoon of sociale media in de les te gebruiken. Tijdens examens, toetsen, overhoringen en proefwerken gelden aangepaste regels.
7. We respecteren elkaars privacy. Bij het gebruik van internet en sociale media worden er daarom geen informatie, foto's of video's verspreid over anderen, als zij daar geen toestemming voor hebben gegeven, of als zij daar negatieve gevolgen van kunnen ondervinden.
8. Internet en sociale media worden alleen gebruikt voor acceptabele doeleinden. Het is daarom niet toegestaan om op school:
 - sites te bezoeken of informatie te downloaden en te verspreiden die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend zijn;
 - hacken en ongeoorloofd toegang te krijgen tot niet-openbare sites of programma's;
 - informatie, foto's of video's te delen waarvan duidelijk is dat die niet bedoeld zijn om verder te verspreiden. Hou je wachtwoorden geheim;
 - verzonnen berichten versturen of een fictieve naam gebruiken als afzender; iemand lastig vallen, te achtervolgen of te 'flamen'.

Als iemand over de voorgaande punten informatie krijgt aangeboden, wordt dat gemeld aan de mentor of de afdelingsleider.

9. Als er gebruik wordt gemaakt van internet en sociale media via van het netwerk van de school, dan mag dat de kwaliteit van het (draadloze) netwerk niet in gevaar brengen of schade aan personen of instellingen veroorzaken. Het hacken, overmatig downloaden of overbelasten van het netwerk is natuurlijk verboden.
10. Leerlingen en medewerkers van CVO 't Gooi worden geen 'vrienden' met elkaar op sociale media, tenzij het gaat om een door de medewerkers gebruikt professioneel account (waar geen persoonlijke informatie over de medewerker op is geplaatst).
11. Als er geconstateerd wordt dat de afspraken niet worden nageleefd, wordt dit eerst met de betrokkene besproken. Bij een ernstige overtreding kan de directie van een van de CVO 't Gooi scholen besluiten een maatregel op te leggen, die kan bestaan uit het in beslag nemen van de telefoon (of vergelijkbare communicatieapparatuur), het uitsluiten van toegang tot het netwerk van de school, het geven van een disciplinaire maatregel (straf) of in het uiterste geval het schorsen of verwijderen van de leerling van school. Hierbij wordt er altijd contact opgenomen met de ouders van de leerling.
Daarnaast kan de directie contact opnemen met de politie indien er sprake is van een strafbaar feit.

Filmen/fotograferen door ouders en leerlingen

Het aantal ouders en leerlingen dat met camera's en smartphones foto's maakt of filmt is in de afgelopen jaren flink toegenomen. Ook deze foto's komen al snel op social media terecht. Ook hier geldt dat een school voor álle kinderen een veilige omgeving moet zijn, en niet een plek waar zij (en hun ouders) het risico lopen ongewenst gefotografeerd te worden. Het maken van foto's en video's door ouders en leerlingen op school kunnen we moeilijk verbieden. We willen er wel afspraken over maken, want een school is niet zomaar een openbare plaats waar iedereen toegang toe krijgt.

We leggen de volgende **afspraken** vast:

1. Wij gaan ervan uit dat iedereen terughoudend is met het maken van foto's en video's en het plaatsen ervan op internet.
2. Het maken van foto's en video's in de school is alleen toegestaan na toestemming van de docent en/of schoolleiding, waarbij de volgende specifieke afspraken gelden:
 - a. Wees terughoudend met het maken van foto's en video's;
 - b. Maak foto's en video's alleen voor eigen gebruik;
 - c. Zet geen foto's en video's van mensen op publiekelijk toegankelijke websites of social media;
 - d. Maak overzichtsfoto's, waar individuele kinderen niet of nauwelijks te herkennen zijn;
 - e. Maak een close-up alleen van jezelf of je eigen kind.

2.11 Verboden handelingen

Het is niet toegestaan om bij wet verboden handelingen uit te voeren op een ict-middel dat voor het volgen van onderwijs en maken van schoolwerk gebruikt wordt. Dit zijn onder andere, maar niet uitsluitend:

- Het opslaan, verspreiden of delen van illegale en/of aanstootgevende bestanden, zoals malware, ransomware en racistisch, discriminerend of beledigend materiaal

- Criminele activiteiten
- Het gebruik van illegale software en/of het omzeilen van licenties
- Inbreken in systemen of accounts van school of andere personen

3. Controle internet en ict-gebruik

De school houdt zich bij controle van het gebruik van internet en ict-middelen aan de geldende wet- en regelgeving, waaronder de Grondwet, Algemene Verordening Gegevensbescherming (AVG), Wet Medezeggenschap Onderwijs (WMO), Burgerlijk Wetboek (BW), Wetboek van Strafrecht.

Onze school gaat bij de controle van internet op school en gebruik van ict-middelen zoals beschreven in deze gedragscode, uit van de juiste balans tussen verantwoord gebruik en bescherming van de privacy van leerlingen.

3.1 Controle op naleving gedragsregels

Voor controle op naleving van deze gedragscode gelden de volgende voorwaarden en afspraken:

- Controle van het gebruik van internet en ict-middelen door leerlingen vindt alleen plaats om de doelen die zijn beschreven in deze gedragscode te bereiken.
- Al het gebruik van internet en ict-middelen zoals beschreven in deze gedragscode wordt automatisch vastgelegd (gelogd), waaronder aanmelding op het netwerk, gebruikte applicaties, bezochte website etc. Deze logbestanden worden na de maximale wettelijke bewaartermijn of eerder vernietigd.
- Controle vindt in beginsel plaats op basis van loggegevens die niet herleidbaar zijn tot identificeerbare personen.
- Niet toegestaan gebruik van internet en ict-middelen wordt zoveel mogelijk technisch onmogelijk gemaakt.
- Door middel van 'meekijksoftware' is het mogelijk dat ict-medewerkers van CVO 't Gooi meekijken met de leerling. Dit kan alleen met toestemming van de leerling, bijvoorbeeld als de leerling problemen heeft met inloggen of gebruik van applicaties. De ict-medewerker kijkt alleen mee met de leerling voor zover dit noodzakelijk is om het probleem op te lossen.
- Om de veiligheid van het netwerk te waarborgen en toe te zien op een zorgvuldig gebruik, worden van tijd tot tijd controles uitgevoerd en wordt er gebruikt gemaakt van monitoring en auditing.
- Als er op basis van deze controles of naar aanleiding van klachten of meldingen een zwaarwegend vermoeden bestaat dat een leerling de regels in deze gedragscode overtreedt, kan er gericht onderzoek plaatsvinden naar het gebruik van internet en ict-middelen door deze leerling.
- Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van het internet en ict-middelen. Als gericht onderzoek nader bewijs oplevert, kan CVO 't Gooi indien dit noodzakelijk is voor het onderzoek ook de inhoud van communicatie of opgeslagen bestanden onderzoeken. Dit kan alleen na schriftelijke toestemming van het bestuur van CVO 't Gooi.

- De leerling en zijn of haar ouders worden zo snel mogelijk geïnformeerd als er een gericht onderzoek plaatsvindt.
- Als het gerichte onderzoek geen aanleiding geeft tot verdere maatregelen worden de bij het onderzoek verzamelde gegevens direct na afronding van het onderzoek vernietigd.

3.2 Controle op plagiaat

Opdrachten van leerlingen kunnen door middel van een gespecialiseerd programma worden gecontroleerd op plagiaat.

4. Sancties

Als een leerling in strijd handelt met deze gedragscode of de algemeen geldende wettelijke regels, kan het schoolbestuur – afhankelijk van de aard en de ernst van de overtreding – disciplinaire maatregelen treffen. Deze disciplinaire maatregelen zijn beschreven in het leerlingenstatuut. Hieronder vallen een waarschuwing, berisping, account-blokkering, schorsing en aangifte bij de politie.

Een leerling die zich niet aan deze gedragscode houdt, wordt zo spoedig mogelijk door de mentor op haar of zijn gedrag aangesproken. De ouders van deze leerlingen worden ook ingelicht. De leerling en diens ouders krijgen daarbij inzage in de vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. De mentor en leerling maken dan afspraken voor de toekomst.

Het schoolbestuur beslist of, en zo ja welke, disciplinaire maatregelen worden opgelegd bij overtreding. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet enkel op basis van een geautomatiseerde gegevens worden getroffen, zoals een constatering van een automatisch filter of blokkade. Er kijkt altijd een persoon mee met de automatisch verzamelde gegevens voordat wordt besloten over disciplinaire maatregelen. Verder worden geen disciplinaire maatregelen getroffen zonder dat de leerling gelegenheid heeft gekregen zijn of haar zienswijze naar voren te brengen.

5. Slotbepaling

Deze regeling wordt periodiek geëvalueerd door de schoolleiding, de GMR en de leerlingenraad.

Het schoolbestuur kan deze gedragscode met instemming van de GMR en de leerlingenraad wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de leerlingen bekend gemaakt.