



Gedragcode ICT en Internet

Leerlingen

Datum instemming CvB & Directie	16 januari 2023
Datum instemming MR	20 april 2023
Plaatsen op P/beleid	✓ Ja
Plaatsen op website	✓ Ja
Bijlage	Infographic
PDCA	3-jaar

1. Inleiding

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

- Hardware, bijvoorbeeld je chromebook, een schoolcomputer of je telefoon
- Software (of systemen), bijvoorbeeld je school google-account en SOMtoday
- Informatie, bijvoorbeeld roosters, e-mails, cijferlijsten en leerlinggegevens

Aan het gebruik van deze middelen zijn risico's verbonden die het stellen van gedragsregels noodzakelijk maken. Hoe jij jouw schoolwerk doet moet veilig zijn en passen binnen wet- en regelgeving. Dit document geeft aan hoe het Cambium College van leerlingen verwacht dat ze omgaan met deze informatie- en communicatiemiddelen.

De afspraken in dit document gelden voor alle plekken waar je je schoolwerk doet en alle informatie- en communicatiemiddelen waar je het werk mee doet. De eerste keer dat een leerling gebruik maakt van het computernetwerk van Cambium College wordt beschouwd als de totstandkoming van een overeenkomst tussen Cambium College en de leerling met betrekking tot dit document, waarbij de leerling instemt met de in dit document verwoorde regels en afspraken.

1 Algemene uitgangspunten

Het document stelt regels ten aanzien van het gebruik van de informatie- en communicatiemiddelen 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.

2 Eigen verantwoordelijkheid en privegebruik

Schoolmiddelen die aan jou zijn toevertrouwd blijven j ouw verantwoordelijkheid. Je dient zorgvuldig om te gaan met door de school beschikbaar gestelde computers, laptops, chromebooks en andere informatie- en communicatiemiddelen. Ook als je bijvoorbeeld je school laptop uitleent aan een andere leerling of wanneer jij je eigen laptop of chromebook, 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 Cambium College beperkt worden 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 of zusjes of je ouders
- Continu 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, palmtops 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 of zelfs een schorsing.

3 *Algemene normen*

Iedere leerling voldoet aan de algemene normen voor 'zorgvuldigheid'. Dit zijn (niet uitputtend):

- Het zorgdragen voor goede fysieke bescherming van alle devices
- Het zorgdragen voor goede technische bescherming van van alle devices
- Het voorkomen van het lekken van interne en vertrouwelijke informatie
- Het voorkomen dat beveiligingsmaatregelen worden omzeild door bijvoorbeeld jailbreaks of hacken
- Het onmiddellijk na constatering melden van verloren of gestolen bedrijfsmiddelen door het sturen van een email aan helpdesk@cambiumcollege.nl

4 *Computergebruik*

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

- Het installeren van software op de computer van Cambium College is niet toegestaan.
- Wachtwoorden zijn persoonlijk en worden niet gedeeld, ook niet incidenteel.
- De leerling sluit na gebruik de computer af of logt uit.
- Bij het tijdelijk verlaten van de werkplek vergrendelt de leerling de computer of laptop
- Iedere leerling heeft de beschikking over eigen opslagdrive om zijn of haar gegevens op te slaan.
- Deze opslagdrive kan worden gescand door de helpdesk op de fysieke aanwezigheid van schadelijke (hack) programma's en inhoudelijk op de aanwezigheid van bestanden met pornografische, racistische, discriminerende, gewelddadige of anderszins onacceptabele, dan wel niet voor het onderwijs aan Cambium 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 (USB stick).

5 *Minimale beveiligingsmaatregelen eigen devices*

Bij het gebruik van eigen devices (chromebook, 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 uitgaan dat Cambium College deze maatregelen hierop ingeregeld heeft.

Voor alle devices moeten minimaal de volgende beveiligingsmaatregelen genomen zijn:

- Bescherm de toegang met een wachtwoord of, in het geval van een smartphone of tablet, met een pincode.
- 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 of pincode vragen.
- Je dient de software up-to-date te houden door periodiek updates te installeren.
- Je dient goede maatregelen tegen virussen of malware te hebben genomen. Bijvoorbeeld door een virus en malware scanner.

Cambium Collegemag controles uitvoeren op bovenstaande maatregelen. Op verzoek van Cambium Collegemoet je zelf aantonen dat de bovenstaande maatregelen worden toegepast.

6 Gebruik van e-mail

Het e-mailsysteem en de bijbehorende mailbox worden aan de leerling voor het uitvoeren van zijn werkzaamheden beschikbaar gesteld. Gebruik van e-mailfaciliteiten is verbonden aan school werkzaamheden en gaan uit van de volgende afspraken:

- De leerling gebruikt voor schoolgerelateerde e-mail het e-mail systeem van het Cambium College
- De leerling gebruikt bij voorkeur voor privémail een externe webmaildienst (zoals Gmail of Hotmail). Privé-gebruik van het school e-mailadres is incidenteel toegestaan.
- 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 11.

7 Gebruik van het computernetwerk van school

Het gebruik van het schoolnetwerk en de bijbehorende faciliteiten worden aan de leerling voor het uitvoeren van de 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 leerlingnetwerk. Na gebruik sluit de leerling zijn eigen account ook weer af.
- De gebruikersnaam en het bijbehorend wachtwoord zijn strikt persoonlijk en mogen niet aan anderen worden doorgegeven.
- De leerling 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, direct contact op te nemen met de helpdesk.
- Het is de leerling 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.

8 Gebruik van internet

Het gebruik van het schoolnetwerk en de bijbehorende faciliteiten worden aan de leerling voor het uitvoeren van de 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 internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten.
- Het is niet toegestaan is 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.

- Het bezoeken van chatboxen of vergelijkbare toepassingen is alleen toegestaan in het kader van lesopdrachten.
- 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.

9 *Gebruik van 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 Cambium 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 Cambium College.

10 *Wachtwoorden en pincodes*

Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en devices (computer, laptop, chromebook of 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 aangegeven tijden vervangen worden.
- Gebruik niet voor elke systeem hetzelfde wachtwoord
- Wachtwoorden zijn persoonlijk en mogen niet gedeeld worden, ook niet incidenteel!

11 *Verboden handelingen*

Het is niet toegestaan om bij wet verboden handelingen uit te voeren op een device wat voor Cambium 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 de beveiliging en licenties

12 Controle

Cambium College handelt binnen de geldende wet- en regelgeving, te weten:

- De Grondwet.
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018).
- algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018).
- Wet Medezeggenschap Onderwijs (WMO).
- Burgerlijk Wetboek (BW).
- Wetboek van Strafrecht.
- Cao VO.

Het Cambium College zal bij controle van het gebruik van informatie en communicatiemiddelen vanuit dit reglement uitgaan van de juiste balans tussen verantwoord gebruik en bescherming van de privacy van leerlingen.

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 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 Cambium College meekijkt met de leerling.
- De leerling 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.
- Opdrachten van leerlingen kunnen door middel van een gespecialiseerd programma worden gecontroleerd op plagiaat.

13 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 door de mentor 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 mentor 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 de leerling gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

Bij Cambium College vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.

Als je een zwakke plek in één van onze systemen heeft gevonden horen wij dit graag zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met je samenwerken om onze leerlingen, medewerkers en onze systemen beter te kunnen beschermen.

Wij vragen jou:

- Je bevindingen te mailen naar helpdesk@cambiumcollege.nl. of deze door te geven aan je mentor of teamleider. De mentor of teamleider zal je vervolgens in contact brengen met onze hoofd ict.
- Het probleem niet te misbruiken door bijvoorbeeld meer informatie te downloaden dan nodig is om het lek aan te tonen of gegevens van andere leerlingen of medewerkers in te kijken, verwijderen of aanpassen,
- Het probleem niet met anderen te delen totdat het is opgelost en alle vertrouwelijke gegevens die zijn verkregen via het lek direct na het dichten van het lek te wissen,
- Geen gebruik te maken van aanvallen op de beveiliging of applicaties van de school,
- Ons als school voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij meer ingewikkelde kwetsbaarheden kan meer nodig zijn.

Wat wij beloven:

- Wij reageren binnen 3 dagen op de melding met onze beoordeling van de melding en een verwachte datum voor een oplossing;
- Als je je aan bovenstaande voorwaarden hebt gehouden zullen wij geen juridische stappen tegen je ondernemen m.b.t. de melding*;
- Wij behandelen jouw melding vertrouwelijk en zullen jouw persoonlijke gegevens niet zonder toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen;
- Wij houden je op de hoogte van de voortgang van het oplossen van het probleem;
- Wij streven er naar om alle problemen zo snel mogelijk op te lossen.

**Ons beleid voor responsible disclosure is geen uitnodiging om onze ict-voorzieningen uitgebreid te scannen om zwakke plekken te ontdekken.*

Er bestaat een kans dt je tijdens jouw 'zoektocht' handelingen uitvoert die volgens de wet of ons schoolbeleid strafbaar zijn. Het doorbreken en binnendringen ('hacken') van de beveiliging van computers, programma's, websites, e.d. is een misdrijf en dus strafbaar. Cambium College zal geen aangifte tegen jou doen, maar dit sluit niet uit dat er mogelijk toch een strafrechtelijk onderzoek naar jouw handelen gedaan kan worden en dat er op basis van dat onderzoek mogelijk strafmaatregelen volgen.