

ICT-reglement

Versie 3.0



Artikel 1 Doel en werkingssfeer van deze regeling, begrippen

- 1.1 Deze regeling geeft de wijze aan waarop binnen het Wartburg College wordt omgegaan met informatie- en communicatietechnologie (ICT). Deze regeling omvat gedragsregels ten aanzien van verantwoord gebruik en geeft regels over de wijze waarop controle plaats vindt.
- 1.2 Onverantwoord gebruik is gebruik tegenstrijdig aan de doelstelling en identiteit van de school, zowel in persoonlijk gebruik als in relatie tot anderen binnen of buiten de school. Hierbij wordt in het bijzonder gedacht aan illegale toepassingen van bestanden, godslasterlijke, beledigende, aanstootgevende, gewelddadige, racistische, discriminerende, intimiderende, pornografische toepassingen, zinloos tijdverdrijf en / of toepassingen die strijdig zijn met de wet of als onethisch te karakteriseren zijn.
- 1.3 De controle op persoonsgegevens bij gebruik van informatie- en communicatietechnologie vindt plaats met als doel:
 - a systeem- en netwerkbeveiliging
 - b tegengaan onverantwoord gebruik.
- 1.4 Deze regeling geldt voor een ieder die ten behoeve van de school werkzaamheden verricht (aangeduid als personeelsleden, maar waaronder ook vallen: stagiaires en vrijwilligers) of onderwijs volgt (leerlingen). Gezamenlijk worden deze in dit reglement ook aangeduid als 'gebruikers'.
- 1.5 Elke nieuwe gebruiker wordt gewezen op de toepasselijkheid van deze regeling. Daarbij wordt aangegeven waar de volledige tekst van deze regeling geraadpleegd/ingezien kan worden.
- 1.6 Voor zover de gebruikers thuis en elders gebruik maken van de ICT (bijvoorbeeld het e-mailadres van school of de schoolwebsites) zijn de bepalingen van deze regeling eveneens van toepassing.
- 1.7 Begripsbepalingen:
 - a schoolleiding: locatiedirectie dan wel het College van Bestuur.
 - b doelstelling en identiteit (van het Wartburg College): de missie en visie van het Wartburg College zoals beschreven in het strategisch beleidskader en zoals ook opgenomen in de schoolgids.
 - c social media: een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Hoofdkenmerken zijn interactie en dialoog tussen de gebruikers.
 - d begeleidingscontact: formeel contact tussen een personeelslid en een leerling gericht op de begeleiding van de leerling bij het onderwijs dat gevolgd wordt aan het Wartburg College.
 - e informatie- en communicatietechnologie (afgekort: ICT): technologie die bestemd is voor het gedigitaliseerd verstrekken en uitwisselen van informatie, met name met behulp van computers, telecommunicatie en informatiesystemen.

Artikel 2 Algemene uitgangspunten

- 2.1 De controle op gebruik van informatie- en communicatietechnologie zal overeenkomstig deze regeling uitgevoerd worden.

- 2.2 Gestreefd wordt naar een goede balans tussen controle op verantwoord gebruik en bescherming van de privacy van personeelsleden en leerlingen.
- 2.3 Persoonsgegevens over gebruik van informatie- en communicatietechnologie worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 6 maanden.
- 2.4 De schoolleiding treft voorzieningen ten aanzien van de positie en integriteit van de ICT-afdeling. Dit wordt geconcretiseerd door de ICT-afdeling alleen technisch verantwoordelijk te laten zijn. De personeelsleden van de ICT-afdeling hebben een geheimhoudingsplicht die inhoudt dat informatie van gebruikers verkregen door het uitvoeren van hun functie nergens anders voor gebruikt wordt. In het bijzonder is het niet toegestaan die informatie te gebruiken voor: privé doeleinden, bij eventuele volgende werkgevers en bij derden.

Artikel 3 Gebruik van informatie- en communicatietechnologie

Verantwoord gebruik

- 3.1 Het gebruik van informatie- en communicatietechnologie is primair verbonden met taken / bezigheden die voortvloeien uit de functie van het personeelslid of het functioneren als leerling.
- 3.2 Gedragsregels die voor personeelsleden gelden voor het ondertekenen van schriftelijke correspondentie, het vertegenwoordigen van de school, het verzenden van post, zijn ook van toepassing bij gebruik van informatie- en communicatietechnologie.
- 3.3 Personeelsleden mogen informatie- en communicatietechnologie beperkt, incidenteel en kortstondig gebruiken voor persoonlijke doeleinden mits dit niet storend is voor de dagelijkse werkzaamheden of het systeem en mits hierbij wordt voldaan aan de verdere regels van deze regeling.
- 3.4 Ten aanzien van de privacy is het privacyreglement van het Wartburg College onverkort van toepassing op de bepalingen in dit ICT-reglement.
- 3.5 Gebruikers van de ICT systemen melden gesignaleerde zwakke plekken in de systemen, zodat zo snel mogelijk maatregelen kunnen worden getroffen. Melding kan worden gedaan bij de functionaris gegevensbescherming (zie verder <https://privacy.wartburg.nl/>).

Onverantwoord gebruik (algemeen)

- 3.6 Het is niet toegestaan om informatie- en communicatietechnologie zodanig te gebruiken dat het systeem- en/of de beveiliging opzettelijk worden aangetast, of de inhoudelijke communicatie tegenstrijdig is aan de doelstelling en identiteit zoals omschreven in artikel 1.2.
- 3.7 Het is niet toegestaan om informatie- en communicatietechnologie voor onacceptabele doeleinden te gebruiken. In het algemeen geldt dat het gebruik van informatie- en communicatietechnologie van de school ten dienste moet staan aan de werkzaamheden of de opleiding van de gebruiker bij het Wartburg College.
- 3.8 Het is in het bijzonder niet toegestaan om:
- a bewust sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
 - b bewust pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal te bekijken of te downloaden of te verspreiden;
 - c zich tot niet-openbare bronnen op het netwerk, internet of andere computernetwerken toegang te verschaffen en het bewust informatie waartoe men via informatie- en communicatietechnologie oneigenlijk toegang heeft verkregen zonder toestemming te veranderen of te vernietigen;
 - d bestanden te downloaden en / of op het computernetwerk of lokaal op een PC te plaatsen die geen verband houden met studie en/of werk;

- e software en applicaties te downloaden en / of te installeren door leerlingen zonder voorafgaande toestemming van de ICT-afdeling;
 - f niet-educatieve spelletjes te spelen;
 - g anoniem of onder een fictieve naam via informatie- en communicatietechnologie te communiceren;
 - h op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende manier via informatie- en communicatietechnologie te communiceren;
 - i inkomende privé-berichten te genereren door het deelnemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, elektronisch winkelen, down- en uploaden van bestanden, nieuwsbrieven en dergelijke;
 - j kettingmailberichten en andere berichten die verstopping veroorzaken of het werk van anderen verstoren te verzenden of door te sturen;
 - k iemand lastig te vallen;
 - l het introduceren en verspreiden van computervirussen en andere software die de integriteit van de gegevens of de computerbeveiliging kunnen beschadigen;
- 3.9 Het is ook anderszins niet toegestaan om door middel van informatie- en communicatietechnologie in strijd met de wet of onethisch te handelen. Het is in het bijzonder verboden om illegale software te installeren en/of te gebruiken.

Toegang tot en gebruik van het interne computernetwerk

- 3.10 Iedere gebruiker heeft recht op toegang tot het computernetwerk en de daarmee verbonden systemen en faciliteiten. Het Wartburg College behoudt zich het recht voor de toegang weer in te trekken.
- 3.11 Gebruikersidentificatie (gebruikersnaam) en authenticatie (bijvoorbeeld wachtwoord en token) worden door de ICT-afdeling verstrekt en zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven.
- 3.12 Het is niet toegestaan zich toegang te verschaffen tot gegevens van andere gebruikers, tenzij met uitdrukkelijke toestemming van de betreffende gebruiker.
- 3.13 Het is gebruiker niet toegestaan om persoonsgegevens die gebruiker ter beschikking staan voor de uitoefening van zijn functie lokaal op te slaan noch op privé-apparatuur, tenzij daarvoor voorafgaande toestemming is verleend door diens leidinggevende en adequate waarborgen zijn getroffen voor de beveiliging van persoonsgegevens. De verantwoordelijkheid voor bestanden die lokaal worden opgeslagen ligt geheel bij de gebruiker. Deze bestanden worden niet veiliggesteld door middel van backup en zijn niet beveiligd tegen misbruik door andere gebruikers.
- 3.14 Leerlingen mogen slechts dan gebruik maken van de ICT-faciliteiten na toestemming van en onder toezicht van personeelsleden.

Gebruik van de ICT-apparatuur

- 3.15 De gebruiker dient zorgvuldig om te gaan met de ICT-apparatuur, zodat deze niet beschadigd raakt. De apparatuur dient in goede orde te worden achtergelaten. Eventuele schade of ontbreken van onderdelen dient direct gemeld te worden aan de ICT-afdeling.
- 3.16 Tijdens het gebruik van de ICT-apparatuur is het niet toegestaan etens- en drinkwaren te nuttigen.
- 3.17 Alleen de ICT-afdeling is bevoegd om apparatuur te ontkoppelen, verplaatsen of aan te sluiten aan het schoolnetwerk of aan apparatuur die aan het schoolnetwerk verbonden is, met uitzondering van het gestelde in artikel 3.19 en 3.20.
- 3.18 De ICT-afdeling verleent alleen ondersteuning op apparatuur die door de ICT-afdeling is aangeschaft en geïnstalleerd.

- 3.19 Het gebruik van eigen USB opslagmedia van de gebruikers is toegestaan onder de volgende voorwaarden:
- a voor het correct laten functioneren van het opslagmedium kan geen beroep worden gedaan op de ICT-afdeling.
 - b de bestanden en programmatuur die op het opslagmedium staan moeten voldoen aan de voorwaarden zoals vastgelegd in het ICT-reglement.
- 3.20 Het gebruik van eigen computerapparatuur in situaties waarin dit noodzakelijk is vanwege een lichamelijke beperking is toegestaan onder de volgende voorwaarden:
- a voor het eerste gebruik wordt contact opgenomen met de ICT-afdeling. Deze is bevoegd om, met opgaaf van redenen, de apparatuur niet toe te staan.
 - b de gebruiker geeft de ICT-afdeling de gelegenheid om voor het eerste gebruik maatregelen te treffen om de beheersbaarheid en de veiligheid te waarborgen.
 - c het gebruik van de betreffende apparatuur moet voldoen aan de voorwaarden zoals vastgelegd in dit reglement.

Toegang tot en gebruik van Internet en e-mail

- 3.21 Toegang tot Internet verloopt uitsluitend via het filtersysteem van zogenaamde blacklisting.
- 3.22 Het is niet toegestaan pogingen te ondernemen om het filtersysteem te omzeilen.
- 3.23 Het versturen van e-mailberichten moet voldoen aan de volgende voorwaarden:
- a de afzender wordt correct weergegeven;
 - b duidelijke onderwerpaanduiding;
 - c terughoudend omgaan met vertrouwelijke gegevens en gevoelige informatie. In het bijzonder dient rekening te worden gehouden met de vereisten ten aanzien van bescherming van persoonsgegevens, zoals vastgelegd in het privacyreglement. Concreet mogen er geen persoonsgegevens worden verstuurd naar derden, tenzij daarvoor een grond is in het privacyregister. Dit mag alleen per mail wanneer het verzonden wordt middels een beveiligd e-mailbericht.

Gebruik van Social media

A. Voor alle betrokkenen (personeelsleden, leerlingen)

- 3.24 Het is personeelsleden niet toegestaan om tijdens de lessen actief te zijn op social media tenzij door de schoolleiding hiervoor toestemming is gegeven. Het is leerlingen niet toegestaan om tijdens de lessen actief te zijn op social media tenzij door onderwijskundige personeelsleden (docenten of onderwijsassistenten) hiervoor toestemming is gegeven.
- 3.25 Het is betrokkenen toegestaan om kennis en informatie te delen, mits het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen niet schaadt.
- 3.26 De betrokkene is persoonlijk verantwoordelijk voor de inhoud welke hij of zij publiceert op de social media.
- 3.27 Elke betrokkene dient zich ervan bewust te zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na verwijdering van het bericht.
- 3.28 Het is voor betrokkenen niet toegestaan om foto-, film- en geluidsopnamen van schoolgerelateerde situaties op de social media te zetten tenzij betrokkenen hier uitdrukkelijk toestemming voor plaatsing hebben gegeven;
- 3.29 Alle betrokkenen nemen de fatsoensnormen in acht. Als fatsoensnormen worden overschreden (bijvoorbeeld: mensen pesten, kwetsen, stalken, bedreigen, zwartmaken of anderszins beschadigen) dan neemt de onderwijsinstelling passende maatregelen. Zie ook artikel 4, 5 en 6.

B. Voor personeelsleden

- 3.30 Het is personeelsleden alleen toegestaan om via social media contacten met leerlingen te onderhouden als zij dat doen op een speciaal daarvoor ingerichte account of pagina waar hij/zij herkenbaar is als personeelslid van het Wartburg College en er sprake is van een begeleidingscontact. Ook in die situaties moet de nodige zorgvuldigheid in acht worden genomen en mag het gebruik van social media geen dwingend karakter hebben.
- 3.31 Personeelsleden dienen zich ervan bewust te zijn dat zij een bijzondere verantwoordelijkheid hebben bij het gebruik van social media: privémeningen van personeelsleden kunnen eenvoudig verward worden met de officiële standpunten van de onderwijsinstelling.
- 3.32 Indien een personeelslid deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met het Wartburg College, dient het personeelslid te vermelden dat hij/zij personeelslid is van het Wartburg College.
- 3.33 Als online communicatie dreigt te ontsporen dient het personeelslid direct contact op te nemen met zijn/haar leidinggevende om de te volgen strategie te bespreken.
- 3.34 Bij twijfel of een publicatie in strijd is met dit reglement neemt het personeelslid contact op met zijn/haar leidinggevende.
- 3.35 Het is het personeelslid toegestaan om schoolgerelateerde onderwerpen te publiceren mits het geen vertrouwelijke of persoonsgebonden informatie over de school, zijn personeelsleden, leerlingen, ouders/verzorgers en andere betrokkenen betreft. Tevens mag de publicatie de naam van de school niet schaden.
- 3.36 Het is voor personeelsleden niet toegestaan standpunten en/of overtuigingen uit te dragen welke in strijd zijn met de doelstelling en identiteit van het Wartburg College en de uitgangspunten van dit reglement.
- 3.37 Indien het personeelslid over het Wartburg College publiceert dient hij/zij het bericht te voorzien van het bericht dat de standpunten en meningen in dit bericht de eigen persoonlijke mening zijn en los staan van eventuele officiële standpunten van het Wartburg College . Verder meldt het personeelslid dat hij of zij niet verantwoordelijk is voor de inhoud en uitlatingen van derden naar aanleiding van of over zijn publicatie.

Artikel 4 Controle (algemeen)

- 4.1 Elke nieuwe gebruiker ontvangt een samenvatting van dit reglement en een verwijzing naar de volledige tekst van dit reglement tegelijk met zijn gebruikersnaam en wachtwoord. Door in te loggen op het interne netwerk accepteert de gebruiker dit reglement.
- 4.2 Controle op gebruik van informatie- en communicatietechnologie vindt slechts plaats in het kader van in artikel 1.2 en 1.3 genoemde doelen.
- 4.3 Controle vindt in beginsel steekproefsgewijs plaats.
- 4.4 Een vermoeden van misbruik van informatie- en communicatietechnologie en inbreuken op de beveiliging, van binnenuit of van buiten de school dienen onmiddellijk aan de ICT-afdeling gemeld te worden.
- 4.5 Ten behoeve van de controle kan de ICT-afdeling gegevens verzamelen en bewaren over het gebruik van de ICT-middelen. Daarbij horen ook de gegevens over de gebruiker en de data en tijdstippen van gebruik.
- 4.6 De schoolleiding kan gebruik maken van de mogelijkheid om door het filtersysteem automatisch gewaarschuwd te worden als een personeelslid of leerling veelvuldig door het filter geblokkeerd wordt. Hierop kan een gerichte controle van het surfgedrag van betrokkene volgen.
- 4.7 De schoolleiding kan de ICT-afdeling verzoeken om een rapportage over het Internet-gebruik.

- 4.8 De schoolleiding kan de ICT-afdeling opdracht geven het computernetwerk te doorzoeken op ongeoorloofde computerbestanden en die te verwijderen.
- 4.9 Personeelsleden mogen in het kader van het toezicht houden op het ICT-gebruik van de leerlingen gebruik maken van systemen om op afstand digitaal inzicht te krijgen in het ICT-gebruik van de leerlingen. Het is niet toegestaan om met dergelijke systemen het ICT-gebruik van personeelsleden te controleren.
- 4.10 Indien de uitlating of gedraging van leerlingen en/of personeelsleden mogelijk een strafrechtelijke overtreding inhoudt kan door het Wartburg College aangifte bij de politie worden gedaan.

Artikel 5 Controle en disciplinaire maatregelen bij leerlingen

- 5.1 Alle leerlingen ontvangen eens per jaar een herinnering aan de geldende regels. Daarbij wordt een samenvatting van de belangrijkste regels gegeven en wordt verwezen naar de volledige tekst van dit reglement.
- 5.2 Als een personeelslid merkt dat het ICT-gedrag van een leerling niet binnen de kaders van dit reglement verloopt, dan spreekt het personeelslid deze leerling hierop aan en meldt dit aan het locatiedirectielid waaronder deze leerling ressorteert.
- 5.3 Indien daartoe aanleiding bestaat kan een locatiedirectielid aan de ICT-afdeling de opdracht geven om de ICT-activiteiten van een leerling na te gaan. Deze opdracht wordt uitgevoerd onder verantwoordelijkheid van de locatiedirectie en onder aansturing van de ICT-afdelingsleider.
- 5.4 In geval van leerlingen die in strijd met dit reglement handelen kan correspondentie omtrent dit onderwerp worden opgenomen in het leerlingendossier.
- 5.5 Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen kan de schoolleiding overgaan tot
 - a het tijdelijk uitsluiten van inlogmogelijkheden voor de betrokken leerlingen, en/of
 - b het melden van dit gedrag en de consequenties aan de ouder(s) / verzorger(s), en/of
 - c het opleggen van een straf / maatregel bijvoorbeeld een waarschuwing of schorsing.

Artikel 6 Controle en disciplinaire maatregelen bij personeelsleden

- 6.1 De schoolleiding informeert de personeelsleden voorafgaand aan de invoering van de regeling over controle op informatie- en communicatietechnologie, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.
- 6.2 Elektronische informatie- en communicatieberichten van de schoolleiding, leden van de Raad van Toezicht, vertrouwenspersonen en andere personeelsleden met een vertrouwensfunctie, gecommuniceerd in het kader van hun functie, zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle bij een ernstig vermoeden van misbruik.
- 6.3 Als een directielid merkt of er op geattendeerd wordt dat het internetgedrag van een personeelslid niet binnen de kaders van dit reglement verloopt, wordt het personeelslid hierop door het directielid gewezen en wordt een controle van zijn internetacties door bevoegde personen als mogelijkheid genoemd.
- 6.4 Het directielid meldt dit aan de direct leidinggevende van het betrokken personeelslid.
- 6.5 Indien daartoe aanleiding bestaat kan een directeur of het College van Bestuur aan de ICT-afdeling de opdracht geven om de ICT-acties van het betrokken personeelslid na te gaan. Deze opdracht wordt uitgevoerd onder verantwoordelijkheid van de directeur of het College van Bestuur en onder aansturing van de ICT-afdelingsleider.

- 6.6 Personeelsleden die in strijd handelen met dit reglement maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het personeelsdossier.
- 6.7 Afhankelijk van de aard of ernst van de uitlatingen, gedragingen en gevolgen kan de directeur of het College van Bestuur overgaan tot:
- a het houden van een gesprek en/of
 - b het geven van een waarschuwing en/of
 - c rechtspositionele maatregelen, welke variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet.
 - d Indien het College van Bestuur de wijze van communiceren door een personeelslid(s) als 'grensoverschrijdend' kwalificeert, dan wordt dit telefonisch gemeld bij de Landelijke Vertrouwensinspecteur (0900 – 1113111).

Artikel 7 Inwerkingtreding en citeertitel

- 7.1 Het College van Bestuur kan dit reglement wijzigen. In die gevallen wordt instemming gevraagd aan de medezeggenschapsraad. Deze wijzigingen worden schriftelijk vastgelegd en voorafgaand aan de invoering aan de personeelsleden en leerlingen bekend gemaakt.
- 7.3 In gevallen waarin dit reglement niet voorziet beslist het College van Bestuur.
- 7.4 Deze regeling kan aangehaald worden als het ICT-reglement of als het Protocol voor het gebruik van e-mail, ICT en sociale media en treedt in werking op 26-3-2019
- 7.5 Het ICT-reglement is vastgesteld door het bevoegd gezag van het Wartburg College op 26-3-2019 en vervangt vorige versies.

Toelichting op het ICT-reglement

Het ICT-reglement betreft het gebruik van internet, e-mail en andere huidige en toekomstige informatie- en communicatietechnologie zoals deze ter beschikking worden gesteld of worden gefinancierd door het Wartburg College. In de tekst wordt hiernaar in algemene zin verwezen als "*informatie- en communicatietechnologie*".

Dit ICT-reglement is afgeleid van de Elektronische informatie- en communicatiemiddelen (EIC)-modelregeling opgesteld door een aantal organisaties voor bestuur en management in het PO en VO, te weten Verus, Bond KBO en Bond KBVO, VBS en VGS. Ten behoeve van het Wartburg College is dit reglement uitgebreid zodat het ook van toepassing is op leerlingen. Ook is gebruik gemaakt van het Protocol Sociale media van Verus.

Een belangrijk punt is de totstandkoming van een goede balans tussen verantwoord gebruik van deze informatie- en communicatietechnologie en bescherming van de privacy van iedereen die op school werkzaamheden verricht en achter de pc zit (dus ook vrijwilligers, stagiaires, enz.). De tekst van dit reglement sluit op dat punt aan bij het privacyreglement van het Wartburg College.

Op grond van art. 7:660 BW is de werkgever gerechtigd tot het geven van voorschriften voor het verrichten van de arbeid en het nemen van maatregelen ter bevordering van de goede orde in de onderneming (in dit geval de school).

Artikelsgewijze toelichting

Artikel 1 Doel van deze regeling

Deze regeling is van toepassing op personen in dienst van of werkzaam voor de school: zij die ten behoeve van de school werkzaamheden verrichten. Hieronder vallen niet alleen de personen die een akte van benoeming/aanstelling hebben, maar ook uitzendkrachten, stagiaires, vrijwilligers, personen die bij de school zijn gedetacheerd, etc. In de tekst wordt geregeld het woord personeelslid gebruikt maar hier worden dus alle personen bedoeld die in dienst zijn van of werkzaamheden ten behoeve van de school verrichten.

Daarnaast is de regeling van toepassing op alle leerlingen. Hieronder vallen alle personen die onderwijs volgen onder verantwoordelijkheid van het Wartburg College en daarbij gebruik maken van de ICT-middelen.

Geregeld wordt in de tekst het woord schoolleiding gebruikt. Hieronder vallen zowel de locatiedirectie als het College van Bestuur. Het zal van de situatie afhangen welk directielid in die situatie de meest aangewezen persoon is om namens de schoolleiding op te treden.

Artikel 2 Algemene uitgangspunten

Lid 2.3

De maximale bewaartermijn van 6 maanden geldt specifiek in het kader van deze regeling; relevante informatie die opgenomen dient te worden in een (personeels)dossier, valt onder de werking van de AVG en kan uit dien hoofde langer worden bewaard. Als er bijvoorbeeld naar aanleiding van een controle reden is om met een personeelslid in gesprek te treden, een waarschuwing te geven, etc. zal dit uiteraard in het personeelsdossier worden vastgelegd.

Lid 2.4

In deze regeling is ervoor gekozen de ICT-afdeling enkel een technische, signalerende verantwoordelijkheid toe te delen. Daarmee kan voorkomen worden dat een systeembeheerder in een loyaliteitsconflict komt met één van zijn collega's. Bij een vermoeden van misbruik van de ICT-middelen van de school wordt het desbetreffende personeelslid door of namens de schoolleiding hierop gewezen; deze taak wordt niet gemandateerd aan ICT-afdeling.

Omdat een systeembeheerder toegang heeft tot bijna alle gegevens binnen het computernetwerk moet de functie met de nodige waarborgen omgeven zijn. Zo heeft hij, net als overigens al het personeel maar op grond van de aard van zijn werkzaamheden in het bijzonder, een geheimhoudingsplicht. Ook is hij niet bevoegd tot het lezen van e-mail of het real-time meekijken zonder dat daartoe een aanleiding is. De systeembeheerder moet tegenover de schoolleiding een

zekere onafhankelijkheid hebben. Hij mag niet door de schoolleiding gedwongen worden af te wijken van procedures die de zorgvuldigheid van het proces bewaken.

Artikel 3 Gebruik van informatie- en communicatietechnologie

Lid 3.3

Een totaal verbod op het privégebruik van informatie- en communicatietechnologie zoals het versturen en ontvangen van persoonlijke e-mailberichten is niet reëel. De school stelt wel beperkende voorwaarden aan het privégebruik.

Lid 3.8

Als de inhoud van een e-mail in ernstige mate ontoelaatbaar is (opruïend, hatelijk, onsmakelijk etc.), of de wet overtreedt (bijvoorbeeld door valse beschuldigingen te doen), zal de schoolleiding contact opnemen met de politie. Print de e-mail uit en bewaar een (digitale) kopie als potentieel bewijsmateriaal. Let op: het adres waar een e-mail vandaan komt is te vervalsen, dus de werkelijke afzender kan zijn/haar identiteit onder iemand anders' naam verborgen houden.

We adviseren om niet te antwoorden op junkmail, omdat de kans groot is dat men er nog meer van ontvangt als men het wel doet. Wees voorzichtig met het bekend maken van het e-mailadres op websites, bijvoorbeeld bij het invullen van een formulier. Ook bij het invullen van het huisadres in publieke gebieden, zoals bijvoorbeeld een 'gastenboek', is voorzichtigheid geboden. Pas op met e-mailberichten waar grote bestanden als attachment zijn bijgevoegd, met name als ze afkomstig zijn van mensen die men niet kent of met onderwerptitels die niets zeggen. Verwijder iedere verdacht bericht en leeg de e-mail prullenbak.

Ad 3.8c) Hier wordt bedoeld op het hacken van systemen, zowel binnen als buiten de school.

Ad 3.8d) Dit artikel gaat over alle soorten bestanden. Het betreft niet alleen het downloaden van bestanden, maar ook het opslaan van bestanden vanaf bijv. een USB-stick.

Hierbij geldt voor personeelsleden wel de nuancering van artikel 3.3 inzake persoonlijk gebruik van de ICT-voorzieningen.

Ad 3.8i) Het gaat hier om het gebruik van het e-mail adres van school voor privé doeleinden. Binnen het gestelde in 3.3 mag een personeelslid op school wel het privé mailadres gebruiken voor privé doeleinden.

Ad 3.8j) Het is leerlingen niet toegestaan e-mailberichten te sturen naar groepen personen, behalve naar de eigen klas of naar kleinere groepen waarmee ze in het kader van het onderwijs samenwerken. Personeelsleden dienen terughoudend te zijn in het sturen van e-mail naar grote groepen mensen. Voor berichten aan grote groepen personeelsleden is het personeelsportaal meestal het meest aangewezen communicatiekanaal. Slechts indien een bericht voor (vrijwel) de gehele groep relevant is en er geen geschikter communicatiekanalen voorhanden zijn, dan kan hiervoor e-mail gebruikt worden. In dat geval dient het bericht geadresseerd te worden aan de afzender (aan-veld) terwijl de rest van de geadresseerden worden opgenomen in het BCC-veld. Hiermee wordt voorkomen dat reacties op het bericht ook weer (onbedoeld) naar grote groepen worden gestuurd.

Lid 3.9

Het installeren en/of gebruiken van illegale software behelst ook het illegaal gebruik van online software. Eventuele aan de school opgelegde boetes hiervoor kunnen door de school worden verhaald op de betrokkene.

Lid 3.10

Onder de faciliteiten die horen bij netwerktoegang, worden gerekend:

- a Mogelijkheid om in te loggen op het computernetwerk
- b Opslagruimte voor persoonlijke bestanden op het computernetwerk, welke ook dagelijks wordt veiliggesteld door de ICT-afdeling middels een backup.
- c E-mailaccount.

De geldigheid van de wachtwoorden wordt door de ICT-afdeling gelimiteerd in tijd. Dit kan verschillen per systeem en per gebruikersgroep, waarbij rekening wordt gehouden met de risico's van misbruik. De gebruiker dient desgevraagd zelf het wachtwoord tijdig te vernieuwen, anders wordt de toegang geblokkeerd.

De hoeveelheid opslagruimte op het computernetwerk per gebruiker wordt door de ICT-afdeling gelimiteerd (zogenoemde quota). De quota kunnen verschillen per systeem en per gebruikersgroep. In bijzondere gevallen kan met opgaaf van redenen via de servicedesk uitbreiding van de grootte van het persoonlijk quotum aangevraagd worden. De ICT-afdeling beslist in die gevallen of uitbreiding realiseerbaar is.

Lid 3.10

Openbaar maken van het wachtwoord kan de integriteit van het netwerk en de daarop aanwezige gegevens schade toebrengen. De gebruiker wordt hier dan ook verantwoordelijk voor gesteld.

Lid 3.15 t/m 3.20

Het doel is om de beschikbaarheid en de bruikbaarheid van de ICT-voorzieningen van het Wartburg College zo hoog mogelijk te laten zijn. Omwille van de beschikbaarheid/beheersbaarheid wordt gebruik van eigen apparatuur in het schoolnetwerk niet toegestaan. Daarbij is rekening gehouden met het feit dat voor steeds meer functies alternatieven beschikbaar zijn, die het gebruik van eigen apparatuur in het schoolnetwerk overbodig maken:

- school e-mail is overal ter wereld te raadplegen;
- bestanden kunnen eenvoudig worden uitgewisseld tussen de privé apparatuur en het schoolnetwerk via de inmiddels wijdverspreide USB-memorysticks of cloud storage diensten;
- steeds meer applicaties komen beschikbaar via een Internet user interface en kunnen dan ook buiten het schoolnetwerk worden gebruikt (SOMtoday, educatieve software)

Voor de goede orde wijzen we er op dat deze regels niet alleen van toepassing zijn op het gebruik van laptops, hoewel daar in de praktijk het meeste vraag naar is. Maar ook het gebruik van eigen mobieltjes, printers, insteekkaarten, webcams, digitale fotocamera's, TV-out apparatuur, CD-branders, scanners etc. vallen hieronder. In het bijzonder, vanwege de extra risicofactor, is het inzetten van eigen netwerkapparatuur (switches, hubs, draadloze access points, modems) en eigen netwerkkabels niet toegestaan. Dit alles met als doel: ervoor te zorgen dat de apparatuur van het Wartburg College het zoveel mogelijk doet en dat de ICT-afdeling beschikbaar is om die apparatuur adequaat te beheren.

Lid 3.20

Het gaat hier alleen om apparatuur die aangesloten wordt op het interne computernetwerk of die indirect verbonden wordt met het interne computernetwerk. Met indirect wordt bedoeld: een apparaat dat aangesloten wordt op bijvoorbeeld een PC van het Wartburg die met het netwerk verbonden is. Eigen apparatuur die gebruikt wordt los van het interne computernetwerk valt niet onder de werking van dit reglement.

Lid 3.22

Onder het omzeilen van het filtersysteem verstaan we alle acties die bedoeld zijn om een website te benaderen die door het filtersysteem geblokkeerd wordt. Hieronder valt bijvoorbeeld het gebruik van zogenaamde anonymous proxy sites. Met instemming van de directie kan incidenteel voor specifieke educatieve toepassingen (zoals een oudercursus Internet) tijdelijk afgeweken worden van deze regel, voor zover dat technisch realiseerbaar is.

Lid 3.23

E-mailberichten die verstuurd worden naar adressen buiten de school worden door het systeem automatisch voorzien van een zogenaamde disclaimer, waarin verwezen wordt naar dit reglement en waarin de verantwoordelijkheid voor de inhoud van de mail bij de afzender wordt gelegd.

Lid 3.24 t/m 3.37 (Social media)

Social media zoals Twitter, Facebook, YouTube en LinkedIn bieden de mogelijkheid om te laten zien dat je trots bent op je school en kunnen een bijdrage leveren aan een positief imago van het Wartburg College. Van belang is te beseffen dat je met berichten op social media (onbewust) de goede naam van de school en betrokkenen ook kunt schaden. Om deze reden vragen wij om bewust met de social media om te gaan.

Essentieel is dat, net als in communicatie in de normale wereld, de school en de gebruikers van social media de reguliere fatsoensnormen in acht blijven nemen en de nieuwe mogelijkheden met een positieve instelling benaderen.

Het Wartburg College vertrouwt erop dat zijn personeelsleden, leerlingen en andere betrokkenen verantwoord om zullen gaan met social media en heeft deze regels opgezet om een ieder die bij het Wartburg College betrokken is of zich daarbij betrokken voelt daarvoor richtlijnen te geven.

Uitgangspunten

1. Het Wartburg College onderkent het belang van social media.
2. Deze regels dragen bij aan een goed en veilig school- en onderwijsklimaat;
3. Deze regels bevorderen dat de instelling, personeelsleden en leerlingen op de social media communiceren in het verlengde van de doelstelling en de identiteit van het Wartburg College en de reguliere fatsoensnormen. In de regel betekent dit dat we respect voor de school en elkaar hebben en iedereen in zijn waarde laten;
4. De gebruikers van social media dienen rekening te houden met de goede naam van de school en van een ieder die betrokken is bij de school;
5. Deze regels dienen de onderwijsinstelling, haar personeelsleden en leerlingen tegen zichzelf en anderen te beschermen tegen de mogelijke negatieve gevolgen van de social media;
6. Het gebruik van social media door de school mag geen dwingend karakter krijgen; leerlingen die niet beschikken over toegang tot social media mogen niet worden buitengesloten.

Doelgroep en reikwijdte

1. Dit reglement is bedoeld voor personeelsleden en leerlingen van het Wartburg College.
2. De regels met betrekking tot social media hebben enkel betrekking op alle berichten die tijdens de lessen worden gepubliceerd, alle schoolgerelateerde berichten of wanneer er een overlap is tussen school, werk en privé.

Artikel 4 Controle

In het algemeen is het streven om niet-toegestaan gebruik van informatie- en communicatietechnologie zo veel mogelijk technisch onmogelijk te maken, voor zover dat het normale gebruik niet al te zeer hindert. Omdat dit nooit volledig sluitend is te maken, is controle op naleving van de regels noodzakelijk.

Lid 4.5

Het personeelslid heeft het recht op inzage in de gegevens. Hij kan verder de werkgever verzoeken de gegevens aan te vullen, te verbeteren, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Tenslotte kan het personeelslid tegen de verwerking van zijn persoonsgegevens verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.

Lid 4.7

In een rapportage over het Internet-gebruik worden onder andere gegevens opgenomen over de voorliggende periode: bezochte websites, geblokkeerde websites, gebruikers die het meest naar geblokkeerde sites zochten. Deze rapportage bevat de gegevens van zowel de leerlingen als de personeelsleden van de betreffende locatie. Op grond van deze algemene rapportage kan de

schoolleiding bij verdenking van misbruik vervolgens om specifieke rapportages vragen, bijvoorbeeld het surfgedrag van een bepaalde gebruiker gedurende een bepaalde periode volledig inzichtelijk maken.

Lid 4.8

Daarbij kan steekproefsgewijs gewerkt worden of gericht gezocht op bepaalde steekwoorden. De ICT-afdeling rapporteert de bevindingen schriftelijk aan de schoolleiding.

Artikel 5 Controle en disciplinaire maatregelen bij leerlingen

Lid 5.3

De ICT-afdeling brengt hiervan schriftelijk verslag uit aan het locatiedirectielid. Ook kan de ICT-afdeling aan de locatiedirectie tijdelijk toegang verstrekken tot de elektronische rapportage van het filtersysteem om inzicht te geven in de bezochte internetsites van de betreffende leerling.

Lid 5.4

De maatregel hangt af van de situatie, de persoon en de ernst en consequenties van de overtreding. Het zal daarom altijd de verantwoordelijkheid zijn van het betreffende locatiedirectielid om te beslissen hoe hiermee om wordt gegaan. In het algemeen is het wel verstandig om hier schoolbreed op vergelijkbare wijze mee om te gaan, om 'rechtsongelijkheid' te voorkomen. Daarbij worden de volgende suggesties voor maatregelen gegeven voor enkele vaker voorkomende overtredingen, waarbij het de taak van het locatiedirectielid is om de ernst van de overtreding te wegen tegen het effect van de maatregel in relatie tot de persoon. Daarbij kan rekening worden gehouden met een eventuele herhaling van overtredingen: hoe vaker een overtreding door de betreffende persoon wordt begaan, hoe strenger de maatregelen die genomen worden.

Hieronder wordt gesuggereerd wat normaliter geëigende maatregelen zouden kunnen zijn. Als er (✓) staat (dus tussen haakjes), dan wordt daarmee bedoeld dat betreffende maatregel in sommige gevallen op zijn plaats kan zijn.

Het opleggen van disciplinaire maatregelen vindt plaats binnen de kaders van het leerlingenstatuut.

Mogelijke maatregelen →	Correctiegesprek	Toegang tijdelijk blokkeren *	Strafwerk / corvee / nablijven	Brief naar ouders	Gesprek met ouders	Toegang permanent blokkeren *	Schadevergoeding	Aangifte politie	Schorsen
<i>Vaker voorkomend onverantwoord ICT-gedrag ↓ (tussen [] staat de verwijzing naar het artikel)</i>									
Misbruik van e-mail, bijv. het (door)sturen van spam, virussen, hoaxes, etc. [3.8]	✓	✓	(✓)						
Misbruik van Internet [3.8] In geval van licht vergrijp (bijv. niet-onderwijskundige sites bezoeken):	✓	✓	✓						
Misbruik van Internet [3.8] In geval van ernstig vergrijp (bijv. pornosites bezoeken)	✓	✓	✓	✓	(✓)				
Hacken (onbevoegd toegang verschaffen tot systemen) in geval van geen of zeer lichte schade. [3.8]	✓	✓	✓	✓	(✓)	(✓)			
Hacken (onbevoegd toegang verschaffen tot systemen) in geval van noemenswaardige schade. [3.8]	✓	✓	✓	✓	✓	✓	✓	(✓)	✓
Digitaal pesten [3.8]	✓	✓	✓	✓	(✓)				
Niet-educatieve spelletjes spelen [3.8]	✓	(✓)							
Kettingmailberichten (mailbom) versturen [3.8]	✓	✓	✓						
Beschadiging aan apparatuur [3.15]	✓	✓	✓	✓	✓	✓	✓		
Eten/drinken nuttigen tijdens PC-gebruik [3.16]	✓	✓	✓				(✓)		

* Het blokkeren van de toegang (tijdelijk of permanent) kan op verschillende niveau's: e-mail, Internet, netwerk of sommige specifieke applicaties. In het algemeen wordt geadviseerd om bij het toepassen van deze maatregel de toegang te blokkeren tot het systeem waarin het onverantwoorde gedrag heeft plaatsgevonden. Dus bij misbruik van e-mail, blokkeren we de toegang tot e-mail.

Artikel 6 Controle en disciplinaire maatregelen bij personeelsleden

Lid 6.2

In beginsel wordt er, ook als er geen vermoeden van misbruik is, steekproefsgewijs gecontroleerd of men zich houdt aan de regels (zie artikel 4.3). Van deze steekproeven zijn de in 6.2 genoemde groepen uitgezonderd omdat zij veelal met zeer vertrouwelijke informatie te maken hebben. Vandaar dat deze groep pas aan controle onderhevig is als er daadwerkelijk een vermoeden van misbruik is. Aan de 'reguliere steekproef' doen zij niet mee. De steekproef is de algemene controle. Er wordt pas gericht (een bepaalde persoon) gecontroleerd als er een vermoeden van misbruik is en in dat geval zijn de genoemde groepen daarvan uiteraard ook niet uitgezonderd en worden zij op dezelfde wijze behandeld als alle andere personeelsleden.

Lid 6.4

Afhankelijk van de ernst van het misbruik wordt de kwestie behandeld door directeur of het College van Bestuur. Als het betrokken personeelslid een locatiedirectielid is, moet de melding altijd worden behandeld door het College van Bestuur. Als het betrokken personeelslid behoort tot het staf- en servicebureau, dan zal in plaats van de directeur de betreffende afdelingsleider worden ingeschakeld.

Lid 6.5

De ICT-afdeling brengt hiervan schriftelijk verslag uit aan de directeur of het College van Bestuur. Ook kan de ICT-afdeling aan de directeur of het College van Bestuur tijdelijk toegang verstrekken tot de elektronische rapportage van het filtersysteem om inzicht te geven in de bezochte internetsites van het betreffende personeelslid.