



Notitie

ICT Gebruiksreglement Medewerkers

22 juni 2017

Bij in dienst treding bij Stichting PrimAH en vanaf het moment dat een medewerker gebruik maakt van ICT-faciliteiten wordt medewerker geacht kennis te hebben genomen van onderstaand ICT-reglement. Elk gebruik in strijd met het in dit ICT reglement bepaalde of zonder de daartoe benodigde afspraken is verboden.

Artikel 1. Definities

In dit ICT gebruiksreglement wordt verstaan onder:

Medewerker

Een ieder die in dienst is van *Stichting PrimAH* dan wel een arbeidsovereenkomst met *Stichting PrimAH* heeft almede een ieder die anderszins in verband met zijn werkzaamheden voor *Stichting PrimAH* gebruik maakt van e-mail-, internet-, telefoonfaciliteiten van *Stichting PrimAH* zoals via externe dienstverleners.

Gebruik

Alle gebruik door medewerkers van de e-mail, internet* en telefoonfaciliteiten van *Stichting PrimAH*.

* Internet: Het World Wide Web en daarmee beschikbare diensten zoals zoekmachines en sociale media maar ook andere protocollen en diensten zoals FTP, Usenet, Skype, etc.

Privédoeleinden

Doeleinden die hun grondslag niet rechtstreeks vinden in de door de medewerker van *Stichting PrimAH* uit te voeren werkzaamheden. Vertrouwelijke informatie waarvan de inhoud strategisch, juridisch, concurrentiegevoelig en/of informatie privacygevoelig van aard is en/of informatie die uitsluitend voor binnen de organisatie bedoeld is.

Artikel 2. Doel van de afspraken

1. Dit reglement geeft de wijze aan waarop binnen *Stichting PrimAH* wordt omgegaan met e-mail-, en internet-, telefoongebruik (hierna: het gebruik) en met de controle van dat gebruik. Deze omvat gedragsregels ten aanzien van verantwoord gebruik en regels over de wijze

waarop controle op het gebruik plaatsvindt.

Stichting PrimAH heeft een gerechtvaardigd belang bij verwerking van de in dit reglement genoemde (persoons)gegevens, te weten een goede interne en externe bedrijfsvoering.

2. De verwerking van persoonsgegevens over het gebruik vindt plaats met als doel:
 - a. Begeleiding en/of individuele beoordelingen
 - b. Bewijs en archivering
 - c. Systeem- en netwerkbeveiliging
 - d. Bescherming van organisatiegeheimen, voorkomen uitlekken vertrouwelijke informatie, voorkomen van negatieve publiciteit
 - e. Tegengaan van seksuele intimidatie of andere vormen van ongeoorloofd gedrag (bv. discriminatie)
 - f. Tegengaan van "verboden gebruik"
 - g. Kosten- en capaciteitsbeheersing

Artikel 3. Algemene uitgangspunten

1. De controle op het gebruik zal in overeenstemming met dit reglement uitgevoerd worden. Indien er zich situaties voordoen waarin dit reglement niet voorziet, zal conform het arbeidsrechtelijke kader en de Wet Bescherming Persoonsgegevens (WBP) en in overleg met de GMR of overlegorgaan gehandeld worden.
2. Ter voorkoming van het lekken van privacygevoelige data zal de medewerker zich houden aan de bepalingen van dit reglement. Tevens zal medewerker zich onthouden van activiteiten waarvan redelijkerwijs bekend is dat deze een onrechtmatige verwerking van persoonsgegevens tot gevolg kunnen hebben.
3. Er wordt gestreefd naar een goede balans tussen controle op gebruik en bescherming van de privacy van medewerkers op de werkplek.
4. Persoonsgegevens over het gebruik worden niet langer bewaard dan noodzakelijk is met het oog op het doel waarvoor de gegevens worden verzameld/verwerkt.

Artikel 4. E-mailgebruik

1. Medewerkers mogen geen gebruik maken van e-mail voor privédoeleinden, tenzij dit binnen de grenzen van de redelijkheid blijft, een en ander ter beoordeling van de leidinggevende, en mits dit niet storend en belemmerend is voor de dagelijkse werkzaamheden en het computernetwerk.
2. Het versturen van e-mailberichten moet voldoen aan de volgende voorwaarden:
 - a. De afzender dient correct vermeld te worden. Het bericht dient ondertekend te zijn met de door *Stichting PrimAH* voorgeschreven handtekening.
3. Het is niet toegestaan om:
 - a. Dreigende, beledigende, seksueel getinte dan wel discriminerende berichten te produceren, te verzenden dan wel door te sturen.
 - b. Zonder toestemming van de verantwoordelijke vertrouwelijke informatie omtrent *Stichting PrimAH* en/of derden te verzenden.
 - c. Kettingbrieven te versturen.
 - d. Berichten te verzenden waarvan de medewerker weet of redelijkerwijs kan vermoeden dat de inhoud hiervan (het imago van) *Stichting PrimAH* kan schaden.
 - e. Mailinglists van *Stichting PrimAH* voor privédoeleinden te gebruiken.
 - f. Beeld- en/of geluidsfragmenten te verzenden, te openen en bekijken/beluisteren indien dit kennelijk voor privédoeleinden geschiedt.
 - g. Anderszins berichten te versturen die op enigerlei wijze *Stichting PrimAH* kunnen benadelen.

Artikel 5. Internetgebruik

1. Medewerkers mogen onder werktijd geen gebruik maken van internet voor privédoeleinden, tenzij dit binnen de grenzen van de redelijkheid blijft, een en ander ter beoordeling van de leidinggevende, en mits dit niet storend en belemmerend is voor de dagelijkse werkzaamheden en het computernetwerk.
2. *Stichting PrimAH* hanteert specifieke schema's voor internet- en computergebruik, welke worden gecontroleerd door het softwareprogramma YourSafetynet. Indien de PC/werkplek van een medewerker is voorzien van YourSafetynet, dient de medewerker zich te houden aan dit schema. Tevens is het de medewerker verboden op enigerlei wijze de controle of restricties opgelegd door YourSafetynet te omzeilen of dit te proberen.
3. Op verzoek wordt een kopie van dit schema aan de medewerker overhandigd.
4. Het is niet toegestaan om:
 - a. Sites te bezoeken die erotisch, pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten.
 - b. Sites te bezoeken die aanzetten tot illegale handelingen waaronder geweld, agressie, gokken en/of alcohol.
 - c. Zonder toestemming van de verantwoordelijke vertrouwelijke informatie over *Stichting PrimAH* en/of derden te verstrekken.
 - d. Op internet in strijd met de wet of onethisch te handelen.
 - e. Software en/of applicaties te downloaden.
 - f. Beeld- en/of geluidsfragmenten te openen en/of op welke wijze dan ook te bewerken indien dit kennelijk voor privédoeleinden geschiedt.
 - g. USB-opslag media (USB-sticks, Foto camera's, MP3 spelers etc.) op het computernetwerk van *Stichting PrimAH* te gebruiken, tenzij medewerker zich er aantoonbaar van heeft verzekerd dat de inhoud van de drager virusvrij is.

Artikel 6. Gebruik en aansluiten eigen client apparatuur (BYOD)

1. Het aansluiten van eigen apparatuur (zoals smartphones, tablets, laptops, etc.) door de medewerker is alleen toegestaan:
 - a. Op de daarvoor beschikbaar gestelde netwerkaansluitingen, waaronder wireless.
 - b. Indien deze voorzien is van wachtwoordbeveiliging, antivirus en anti-malware software.
 - c. Indien de meegebrachte apparatuur voorzien is van legitiem geïnstalleerde software en geldige licentie(s). In geval van twijfel dient de medewerker de geldigheid te verifiëren bij de software leverancier. In geval van overtreding van het vorenstaande, is de medewerker jegens *Stichting PrimAH* schadelijkt. De medewerker zal *Stichting PrimAH* vrijwaren van aanspraken die derde partijen op *Stichting PrimAH* mochten menen te hebben uit gevolg van de voornoemde overtredingen.
2. Medewerker zal alleen schoolvertrouwelijke informatie verwerken op deze apparatuur als dat onvermijdelijk is gezien de aard van de informatie (bv. e-mail met bijlagen) of als door *Stichting PrimAH* expliciet aangegeven is dat deze informatie op dergelijke apparatuur gebruikt mag worden.

Artikel 7. Telefoongebruik

1. Medewerkers mogen geen gebruik maken van de telefoon (vast/mobiel) voor privédoeleinden, tenzij dit binnen de grenzen van de redelijkheid blijft, een en ander ter beoordeling van de leidinggevende.

2. Het is niet toegestaan om:
 - a. Dreigende, beledigende, seksueel getinte dan wel discriminerende gesprekken te voeren, uitspraken te doen en/of sms-berichten te sturen.
 - b. Zonder toestemming van de verantwoordelijke vertrouwelijke informatie omtrent *Stichting PrimAH* en/of derden te verstrekken.
 - c. Mededelingen te doen en/of per tekstbericht informatie te verstrekken waarvan de medewerker weet of redelijkerwijs kan vermoeden dat de inhoud hiervan (het imago van) *Stichting PrimAH* kan schaden.
 - d. Telefoonlijsten van het *Stichting PrimAH* voor privédoeleinden te gebruiken.
 - e. Zogenaamde betaalnummers te bellen, tenzij dit m.b.t. de werkzaamheden noodzakelijk is.
 - f. Naar het buitenland te bellen, tenzij en voor zover dit noodzakelijk is m.b.t. voor de werkzaamheden.
 - g. Sms-berichten te sturen naar zogenaamde betaalnummers.
3. Indien de telefoon beschikt over smartphone-capaciteiten, e-mail en/of internettoegang, dan gelden artikel 4 en 5 ook voor e-mail en internetgebruik middels deze telefoon. Tevens geldt bij internetgebruik middels de telefoon een verbod op het overschrijden van datalimieten gesteld door de provider.

Artikel 8. Vertrouwelijke informatie

1. Het zonder toestemming van de verantwoordelijke aan derden verstrekken van vertrouwelijke informatie (ook indien dit op andere wijzen dan via e-mail, internet, fax, telefoon en/of post geschiedt) is niet toegestaan. *Stichting PrimAH* kan op basis van schending van het voorgaande verbod, overgaan tot het treffen van (disciplinaire) rechtsmaatregelen.
2. Medewerkers die vanuit een andere dan de vaste werkplek hun werkzaamheden uitvoeren, doen al hetgeen redelijkerwijs van hen verwacht mag worden om vertrouwelijk met de aan hen uit hoofde van hun werkzaamheden beschikbaar staande gegevens om te gaan.
3. Een medewerker die een (vermoedelijke) schending van de in het voorgaande leden bedoelde gedragsregels waarneemt, meldt dit terstond aan de leidinggevende van de medewerker die de gedragsregels geacht wordt te hebben geschonden.
4. *Stichting PrimAH* heeft op het netwerk voor verschillende afdelingen een algemene plaats ingeruimd om bestanden, die geen vertrouwelijke informatie bevatten, onderling uit te wisselen. Vertrouwelijke informatie mag niet via dit systeem worden uitgewisseld.

Artikel 9. Controle

1. Controle op het gebruik vindt slechts plaats in het kader van in artikel 2.2 genoemde doelen. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle:
 - a. In het kader van begeleiding en/of individuele beoordelingen kan steekproefsgewijs controle plaatsvinden van zakelijke e-mailberichten en/of poststukken, alsmede van zakelijk telefoonverkeer. Van telefoongesprekken kan tevens een opname gemaakt worden. Het voorgaande geschiedt zoals vooraf overeengekomen met de individuele medewerker.
 - b. Conform de bedrijfsregels kan er door de medewerker zelf en/of de daartoe aangewezen en vooraf aan de medewerker bekend gemaakte functionaris een kopie gemaakt worden van de zakelijke e-mailberichten en/of poststukken. Tevens kan er een opname gemaakt worden van zakelijke telefoongesprekken. In beide voorgaande gevallen geschiedt dit met als doel bewijs en/of archivering.

- c. Voor het tegengaan van virussen en andere schadelijke programma's, in het kader van systeem- en netwerkbeveiliging, kan e-mail en internetgebruik op geautomatiseerde wijze worden gecontroleerd.
 - d. Controle op het uitlekken van organisatiegeheimen en/of anderszins vertrouwelijke informatie kan plaatsvinden op basis van steekproefsgewijze inhoudsfiltering, dan wel door gerichte controle indien inhoudsfiltering niet mogelijk is en er reeds een gerechtvaardigd vermoeden bestaat. Een verdacht e-mail bericht wordt apart gezet voor nader onderzoek.
 - e. Controle in het kader van het voorkomen van negatieve publiciteit kan plaatsvinden op basis van inhoudsfiltering. Verdachte berichten worden geautomatiseerd terug gestuurd naar de afzender en "verboden" sites geblokkeerd. Tevens kunnen in dit kader gerichte controles plaatsvinden van poststukken, fax- en telefoonverkeer, indien er reeds een gerechtvaardigd vermoeden bestaat.
 - f. Controle in het kader van het tegengaan van seksuele intimidatie of andere vormen van ongeoorloofd gedrag (bv. discriminatie) kan op geautomatiseerde wijze plaatsvinden. Verdachte berichten worden geautomatiseerd terug gestuurd naar de afzender.
 - g. Controle in het kader van het tegengaan van "verboden gebruik" vindt in beginsel geanonimiseerd en slechts steekproefsgewijs plaats.
 - h. Controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeersgegevens (tijd, hoeveelheid, omvang, etc.).
2. Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een medewerker of een groep medewerkers ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaats vinden.
 3. Controle beperkt zich in principe tot verkeersgegevens van het gebruik. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats.
 4. Medewerkers ten aanzien van wie geconstateerd is dat zij zich niet aan dit reglement houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken en uitgenodigd voor een gesprek.
 5. In geval van strafbaar internetgebruik, kan *Stichting PrimAH* hiervan aangifte doen.
 6. E-mailberichten en telefoongesprekken en poststukken van MR-leden, en andere medewerkers met een vertrouwensfunctie ten opzichte van medewerkers van *Stichting PrimAH* zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het berichtenverkeer.
 7. Het is de werkgever in beginsel toegestaan de vastgelegde gegevens ten aanzien van het gebruik van elektronische communicatiemiddelen te analyseren ten behoeve van het onderzoeken van ongeoorloofd gedrag indien er sprake is van een redelijke verdenking of vermoeden van een ongeoorloofde handeling door één of meerdere werknemers. Hierbij wordt ervan uitgegaan dat andere middelen zijn uitgeput, dat er een zwaarwichtig belang van de schoolorganisatie in het geding is en dat bij de uitvoering rekening wordt gehouden met de ernst van de gevolgen voor de betrokken werknemer(s) en de wijze waarop in de bescherming van de privacy van de werknemers wordt voorzien. De betreffende gegevens worden bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een gebruiker noodzakelijk is.

Artikel 11. Rechten van de betrokkenen

1. *Stichting PrimAH* informeert de medewerkers over de invoering van dit reglement, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van dit reglement. (zie artikel 33, WBP).

2. De medewerker kan zich tot *Stichting PrimAH* wenden met het verzoek om een volledig overzicht van zijn verwerkte persoonsgegevens. Het verzoek wordt binnen 4 weken beantwoord. (zie artikel 35, WBP).
3. De medewerker kan verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend, dan wel in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek wordt binnen 4 weken beantwoord. (zie artikel 36, WBP)).
4. De medewerker kan bij *Stichting PrimAH* verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. *Stichting PrimAH* oordeelt binnen 4 weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien *Stichting PrimAH* het verzet gerechtvaardigd acht, beëindigt *Stichting PrimAH* terstond de verwerking. (zie artikel 40, WBP).

Artikel 12. Klachten

1. Indien de medewerker meent benadeeld te zijn in zijn rechten als gevolg van dit reglement, dan kan hij zich richten tot *Stichting PrimAH*. Zijn klacht wordt binnen een zo kort mogelijke termijn als redelijk is, vertrouwelijk behandeld.

Artikel 13. Slotbepaling

1. Dit reglement laat elke uit wet, CAO of andere geldende regeling voortvloeiende bevoegdheid of voorziening voor de Ondernemingsraad, Medezeggenschapsraad en/of *Stichting PrimAH* onaangetast.
2. *Stichting PrimAH* en de Gemeenschappelijke Medezeggenschapsraad (GMR) kunnen dit reglement in onderling overleg wijzigen of aanpassen. Aanpassingen of wijzigingen worden schriftelijk vastgelegd en door *Stichting PrimAH* en de Gemeenschappelijke Medezeggenschapsraad (GMR) ondertekend en vervolgens aan de medewerkers bekend gemaakt.
3. In het geval van onvoorziene omstandigheden, is *Stichting PrimAH* gerechtigd van dit reglement af te wijken, een en ander slechts indien er sprake is van een direct en zwaarwegend belang voor *Stichting PrimAH*. De voorzitter van de Gemeenschappelijke Medezeggenschapsraad (GMR) zal onmiddellijk van vorenbedoelde omstandigheid in kennis worden gesteld.
4. Het reglement is geldig vanaf het moment dat deze overeenkomst akkoord is bevonden en wordt daarna steeds met een periode van één jaar stilzwijgend verlengd, tenzij *Stichting PrimAH* of de Gemeenschappelijke Medezeggenschapsraad (GMR) ten minste één maand voor het verstrijken van de periode van één jaar, schriftelijk aan de andere partijen heeft aangegeven het reglement te willen wijzigen of beëindigen.
5. Indien wetgeving of maatschappelijke ontwikkelingen daartoe aanleiding geven, treden *Stichting PrimAH* en de Gemeenschappelijke Medezeggenschapsraad (GMR) met elkaar in overleg inzake eventuele aanpassingen van dit reglement.

Artikel 14. Algemeen

Onvoorziene situaties

In situaties waarin deze regeling niet voorziet, zal door *Stichting PrimAH* zoveel mogelijk naar aard en strekking van hetgeen in dit reglement is geregeld in redelijkheid worden beslist.

Inwerkingtreding

Dit reglement zal in werking treden op *1 juli 2017*. Alle voordien gehanteerde regelingen, gebruiken en afspraken vervallen met ingang van de invoeringsdatum.