



Stichting PrimAH

November 2026

Reglement voor het gebruik van ICT en Social Media



Openbaar Primair Onderwijs AA en Hunze

Inhoudsopgave

Inhoud

Inhoudsopgave	2
Artikel 1 – Toepassing en kennisname	3
Artikel 2 – Definities	3
Artikel 3 – Doel van dit reglement	3
Artikel 4 – Algemene uitgangspunten.....	4
Artikel 5 – Communicatiediensten (e-mail, ouderportaal)	5
Artikel 6 – Netwerk- en Internetgebruik.....	5
Artikel 7 – Eigen apparatuur (BYOD)	6
Artikel 8 – Werken buiten PrimAH.....	6
Artikel 9 – Telefoongebruik.....	7
Artikel 10 – Sociale media door personeel (privégebruik).....	8
Artikel 11 – Social media door de school	9
Artikel 12 – Gebruik van AI-toepassingen.....	9
Artikel 13 – Websites van de scholen.....	9
Artikel 14 – Instant messaging (IM)	10
Artikel 15 – Vertrouwelijke informatie	11
Artikel 16 – Controle	11
Artikel 17 – Rechten van betrokkenen.....	12
Artikel 18 – Klachten.....	13
Artikel 19 – Slotbepalingen	13
Artikel 20 – Algemeen	13

Artikel 1 – Toepassing en kennisname

Het gebruik van diverse ICT-faciliteiten en het gebruik van Sociale Media is in onze moderne samenleving niet meer weg te denken. Het speelt een dagelijkse rol in het leven van ons allemaal. Het gebruik van ICT-faciliteiten en Sociale Media, al dan niet uit naam van de school, vraagt om heldere afspraken. Om die reden is dit reglement tot stand gekomen.

Vanaf het moment dat je in dienst komt bij Stichting PrimAH, verwachten we dat je dit reglement hebt gelezen en naleeft. Elk gebruik dat in strijd is met dit reglement, of zonder de benodigde afspraken, is niet toegestaan.

Artikel 2 – Definities

Medewerker

Iedereen die bij Stichting PrimAH een arbeids- of stageovereenkomst heeft, én iedereen die voor werkzaamheden voor Stichting PrimAH gebruikmaakt van e-mail, internet of telefoondiensten van (of via) Stichting PrimAH, ook via externe dienstverleners.

Gebruik

Al het gebruik door medewerkers van e-mail-, internet*- en telefoonfaciliteiten van Stichting PrimAH.

* **Internet:** het World Wide Web en diensten zoals zoekmachines en sociale media, maar ook andere door Stichting PrimAH gebruikte applicaties zoals Social Schools, Cloudwise, ParnasSys, etc.

Privédoeleinden

Doeleinden die niet rechtstreeks horen bij je werk voor Stichting PrimAH.

Vertrouwelijke informatie

Informatie die strategisch, juridisch, concurrentie- en/of privacygevoelig is, en/of uitsluitend bedoeld is voor intern gebruik.

Artikel 3 – Doel van dit reglement

1. Dit reglement legt vast hoe binnen Stichting PrimAH wordt omgegaan met software, e-mail, internet, telefonie en social media gebruik dat verband houdt met de schoolactiviteiten van Stichting PrimAH (hierna: **het gebruik**) en hoe controle daarop plaatsvindt. Het bevat gedragsregels en afspraken voor verantwoord gebruik en regels voor controle. Stichting PrimAH heeft hierbij een gerechtvaardigd belang: een goede interne en externe bedrijfsvoering.

Persoonsgegevens over het gebruik worden verwerkt met de volgende doelen:

- a. Begeleiding en/of individuele beoordelingen
- b. Bewijs en archivering
- c. Systeem- en netwerkbeveiliging
- d. Bescherming van organisatiegeheimen; voorkomen van uitlekken van vertrouwelijke informatie; voorkomen van negatieve publiciteit
- e. Tegengaan van seksuele intimidatie of andere ongeoorloofde vormen van gedrag (bijv. discriminatie)
- f. Tegengaan van **verboden gebruik**
- g. Kosten- en capaciteitsbeheersing

Artikel 4 – Algemene uitgangspunten

1. Controle op gebruik gebeurt volgens dit reglement. In situaties die niet zijn voorzien, handelen we binnen het arbeidsrechtelijke kader en de Wet bescherming persoonsgegevens (Wbp) en in overleg met de GMR of een (extern) overlegorgaan.
2. Om lekken van privacygevoelige data te voorkomen, houd je je aan dit reglement en laat je activiteiten achterwege waarvan je redelijkerwijs weet dat ze kunnen leiden tot onrechtmatige verwerking van persoonsgegevens.
3. We streven naar een goede balans tussen controle en jouw privacy op de werkplek.
4. Persoonsgegevens over het gebruik worden niet langer bewaard dan nodig is voor het doel waarvoor ze zijn verzameld.

Artikel 5 – Communicatiediensten (e-mail, ouderportaal)

1. Privégebruik voor het versturen van berichten via e-mail en/of het ouderportaal is niet toegestaan, behalve als het binnen redelijke grenzen blijft, niet stoort of belemmert, en je leidinggevende hier toestemming voor geeft. Het mag het computernetwerk niet belasten. Je gebruikt je privé e-mail niet voor je werk.

Voorwaarden voor verzenden:

- a. Vermeld de afzender correct en gebruik de door Stichting PrimAH voorgeschreven e-mailhandtekening.
- b. Een e-mail – al dan niet met bijlage(n) - met vertrouwelijke of gevoelige inhoud en/of persoonsgegevens bestemd voor een externe partij buiten Stichting PrimAH, wordt altijd beveiligd verstuurd met behulp van e-mailbeveiligingssoftware (bijvoorbeeld Zivver).

Het is verboden om:

- a. Dreigende, beledigende, seksueel getinte of discriminerende berichten te (laten) maken, verzenden of doorsturen.
- b. Zonder toestemming vertrouwelijke informatie van of over Stichting PrimAH en/of derden te verzenden.
- c. Kettingbrieven te versturen.
- d. Berichten te verzenden waarvan je weet of kunt vermoeden dat ze het imago van Stichting PrimAH kunnen schaden of benadelen. Op welke manier dan ook.
- e. Mailinglijsten van Stichting PrimAH voor privédoeleinden te gebruiken.
- f. Beeld-/geluidsfragmenten te verzenden, openen of bekijken/beluisteren als dat duidelijk privé is.

Artikel 6 – Netwerk- en Internetgebruik

1. Zakelijke ICT-voorzieningen en internetverbindingen zijn primair bestemd voor werk- en onderwijs gerelateerde doeleinden. Kortstondig privégebruik is uitsluitend toegestaan buiten de uren of geplande werktaken (zoals in de pauze), mits dit de werkzaamheden niet verstoort en de netwerkcapaciteit niet belast.

Het is verboden om:

- a. Sites te bezoeken met erotisch, pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal.
- b. Sites te bezoeken die aanzetten tot illegale handelingen, zoals geweld, agressie, gokken en/of alcoholmisbruik.
- c. Zonder toestemming persoonsgegevens en/of vertrouwelijke informatie over Stichting PrimAH aan derden te verstrekken.
- d. In strijd met de wet of onethisch te handelen op internet.
- e. Software en/of applicaties te downloaden, zonder expliciete toestemming.
- f. Beeld-/geluidsfragmenten te openen/bewerken als dat duidelijk privé is.
- g. USB-opslagmedia (USB-sticks, fotocamera's, MP3-spelers, etc.) op het netwerk te gebruiken, tenzij je aantoonbaar hebt gecontroleerd dat ze virusvrij zijn.

Artikel 7 – Eigen apparatuur (BYOD)

1. Het aansluiten van eigen apparaten (smartphone, tablet, laptop, etc.) mag alleen:
 - a. Op aangewezen netwerkaansluitingen (incl. wireless).
 - b. Als het apparaat is beveiligd met wachtwoord, voorzien van antivirus en anti-malwaresoftware en door de fabrikant ondersteund wordt met beveiligingsupdates.
 - c. Als alle software legaal is geïnstalleerd en geldig is gelicentieerd. Bij twijfel verifieer je dit bij de leverancier. Bij overtreding ben je schadeplichtig tegenover Stichting PrimAH en vrijwaar je Stichting PrimAH tegen aanspraken van derden.
2. Het verwerken van school-vertrouwelijke informatie op eigen apparatuur is niet toegestaan. Je gebruikt alleen de door Stichting PrimAH beschikbaar gestelde devices. Uitzondering hierop is het gebruik van een applicatie op mobiele telefoon ten behoeve van e-mail en/of het ouderportaal.

Artikel 8 – Werken buiten PrimAH

Ter voorkoming van datalekken en ongeoorloofde toegang tot schoolgegevens, is de medewerker gehouden aan strikte voorschriften met betrekking tot het verbindingsgedrag. Hierbij wordt onderscheid gemaakt tussen de volgende drie situaties:

1. Gebruik van de thuiswerkplek

De medewerker draagt de volledige verantwoordelijkheid voor de basisveiligheid van het private netwerk. Gebruik van schoolapparatuur via een thuisnetwerk is uitsluitend toegestaan indien voldaan wordt aan de volgende technische randvoorwaarden:

- a. Encryptie: Het draadloze netwerk (Wi-Fi) dient minimaal te zijn beveiligd middels het WPA2- of WPA3-protocol met een uniek, sterk wachtwoord.
- b. Toegangsbeheer: De door de provider ingestelde standaard inloggegevens (zoals 'admin' of '1234') van de router/modem moeten aantoonbaar zijn gewijzigd.
- c. Patchmanagement: De firmware van de netwerkapparatuur dient actueel te zijn door het (automatisch) installeren van beschikbare beveiligingsupdates.

2. Werken op locaties van derden (Partners en Relaties)

Indien werkzaamheden worden verricht op locatie bij een externe partner of relatie, is het gebruik van het daar aanwezige (gasten)netwerk toegestaan.

- a. Indien toegang wordt verkregen via individuele, geautoriseerde inloggegevens. Dus niet publiekelijk bekend.
- b. Bij enige onduidelijkheid over de integriteit of beveiliging van het betreffende netwerk, is het niet toegestaan om verbinding te maken. Het gebruik van een 4G/5G-hotspot is dan verplicht.

3. Werken op openbare locaties

Netwerken op openbare locaties (zoals horeca, hotels en treinstations) worden aangemerkt als inherent onveilig. Dit geldt expliciet ook voor netwerken waarvan het wachtwoord publiekelijk toegankelijk is.

- a. Het is niet toegestaan om verbinding te maken met een openbaar netwerk. Het gebruik van een 4G/5G-hotspot is dan verplicht.

4. Werken en apparatuur in het buitenland

- a. Het meenemen en gebruiken van door Stichting PrimAH ter beschikking gestelde apparatuur (laptops, tablets, telefoons) buiten Nederland is in beginsel **niet toegestaan**.
- b. Uitzondering op het eerste lid geldt uitsluitend voor medewerkers in de functie van *bestuurder, schoolleider, bovenscholts ict'er, privacy officer* of medewerkers die voor hun specifieke functie/dienstreis aantoonbaar werkzaamheden in het buitenland moeten verrichten.
- c. Indien het meenemen van apparatuur naar het buitenland noodzakelijk is:
 1. Dient dit vooraf te worden gemeld bij de leidinggevende én de IT-afdeling;
 2. Blijven alle beveiligingsvoorschriften uit dit artikel (zoals het verbod op openbare Wi-Fi en verplicht gebruik van MFA) onverkort van kracht;
 3. Is het verwerken van persoonsgegevens buiten de Europese Economische Ruimte (EER) uitsluitend toegestaan na expliciete goedkeuring van de Privacy Officer.

Artikel 9 – Telefoongebruik

1. Privégebruik (vast/mobiel) is niet toegestaan, behalve als het binnen redelijke grenzen blijft en je leidinggevende dit toestaat.

Het is verboden om:

- a. Dreigende, beledigende, seksueel getinte of discriminerende uitlatingen te doen of sms'jes te sturen.
 - b. Zonder toestemming vertrouwelijke informatie van of over Stichting PrimAH en/of derden te verstrekken.
 - c. Mededelingen te doen of berichten te sturen die het imago van Stichting PrimAH kunnen schaden.
 - d. Telefoonlijsten van Stichting PrimAH privé te gebruiken.
 - e. Betaalnummers te bellen, tenzij dit noodzakelijk is voor je werk.
 - f. Naar het buitenland te bellen, tenzij dit noodzakelijk is voor je werk.
 - g. Betaal-sms'jes te versturen.
2. Heeft de telefoon e-mail en/of internetmogelijkheden? Dan gelden ook artikel 5 en 6. Daarnaast mag je datalimieten van de provider niet overschrijden.

Artikel 10 – Sociale media door personeel (privégebruik)

1. Onder sociale media verstaan we alle onlinemogelijkheden om te communiceren en informatie te delen, zoals X (Twitter), Facebook, LinkedIn, Slideshare, YouTube, WhatsApp, Snapchat, Instagram, Life, etc. Kenmerken kunnen zijn:
 - a. Informatie (tekst, foto, video) kan zich razendsnel wereldwijd verspreiden.
 - b. Informatie is moeilijk of niet te verwijderen en kan door anderen makkelijk worden opgeslagen.
 - c. Je kunt chatten, discussiëren, nieuws/informatie verspreiden en kennis opdoen/delen.
2. Bij het gebruik van social media dienen de volgende aandachtspunten in acht genomen te worden:
 - a. Wees je ervan bewust dat uitingen op sociale media voor onbepaalde tijd openbaar kunnen blijven, ook na verwijderen. Denk dus goed na voordat je iets plaatst.
 - b. Presenteer alleen feiten die je met geverifieerde bronnen kunt onderbouwen.
 - c. Berichten zijn vaak openbaar en bereiken snel veel mensen. Ouders, leerlingen, collega's en leveranciers maken meestal geen onderscheid tussen persoonlijke en zakelijke profielen. Gedraag je daarom altijd professioneel.
 - d. Houd rekening met de reputatie van Stichting PrimAH en iedereen die daarbij betrokken is.
 - e. Overschrijd normale fatsoensnormen niet: geen pesten, kwetsen, beledigen, zwartmaken, stalken of bedreigen; geen vulgair/obsceen materiaal (zoals pornografisch of discriminerend).
 - f. Ideeën bespreken mag, maar roddelen over personen hoort niet op sociale media.
 - g. Raak niet verward in ruzies of discussies; laat je niet verleiden tot persoonlijke aanvallen.
 - h. Bekritiseer geen andere scholen of organisaties.
 - i. Verspreid geen spam.
 - j. Foto-, film- en geluidsopnamen van werksituaties plaats je alleen met uitdrukkelijke toestemming van betrokkenen én als zij daardoor niet worden geschaad.
 - k. Publiceer geen werken van anderen (zoals foto's of teksten) zonder toestemming; dit kan in strijd zijn met rechten van anderen en Stichting PrimAH schaden.
 - l. Deel nooit vertrouwelijke informatie via sociale media, zoals persoonsgegevens van leerlingen/collega's/medewerkers, financiële informatie of intellectuele eigendom van Stichting PrimAH.
 - m. Je bent zelf verantwoordelijk voor alles wat je plaatst. Ook doorsturen (forwarden) en herplaatsen (bijv. retweeten) valt hieronder.
 - n. Bij twijfel: niet plaatsen. Voel je vrij om eventueel contact op te nemen met de schooldirecteur of de privacy officer voor advies.
 - o. Overtreed je deze regels, dan word je daarop aangesproken. Alle correspondentie hierover wordt in je personeelsdossier opgenomen.
 - p. Als uitingen mogelijk een strafbaar feit vormen, kan Stichting PrimAH aangifte doen.
 - q. Afhankelijk van de ernst kunnen maatregelen volgen: van waarschuwing tot ontslag.

Artikel 11 – Social media door de school

De scholen van Stichting PrimAH maken geen gebruik van Sociale Media-kanalen. Dit ter bescherming van de digitale identiteit van onze leerlingen en medewerkers. We voorkomen hiermee imagoschade, juridische risico's en onnodige inbreuk op de persoonlijke levenssfeer.

Algemene informatie, nieuws en activiteiten worden alleen gedeeld met de betrokken ouders in het daarvoor bedoelde ouderportaal.

Artikel 12 – Gebruik van AI-toepassingen

1. Bij het gebruik van netwerken, apparatuur en cloudomgevingen van Stichting PrimAH is de inzet van Artificial Intelligence (AI) en generatieve AI-tools uitsluitend toegestaan mits voldaan wordt aan de kaders uit het AI-beleid van Stichting PrimAH.
2. Het is medewerkers niet toegestaan om (bijzondere) persoonsgegevens, vertrouwelijke schoolinformatie of auteursrechtelijk beschermd materiaal in te voeren in openbare of niet door de stichting goedgekeurde AI-systemen.
3. Voor de goedgekeurde AI-tools, richtlijnen en verantwoord gebruik wordt verwezen naar het geldende AI-beleid van Stichting PrimAH.

Artikel 13 – Websites van de scholen

Alle scholen en het bestuurskantoor van Stichting PrimAH beschikken over een eigen website met een eigen domeinnaam. De websites worden gehost bij onze ICT-partner. Het beheer is volledig in handen van Stichting PrimAH.

1. De schoolwebsite dient uitsluitend als officieel informatiekanaal voor huidige ouders/verzorgers, potentiële nieuwe ouders en externe belanghebbenden. De website heeft een informatief en faciliterend karakter.
2. De website wordt gebruikt voor het ontsluiten van wettelijk verplichte en schoolspecifieke documenten, waaronder in ieder geval de schoolgids, het schoolplan en het jaarverslag. Daarnaast kunnen er algemene nieuwtjes, aankondigingen van activiteiten en kalenderinformatie worden gedeeld.
3. Om de eenheid en professionele uitstraling van Stichting PrimAH te waarborgen, maken alle scholen gebruik van een uniform website-sjabloon. Het is scholen niet toegestaan om eigenhandig wijzigingen aan te brengen in de technische structuur, de grafische opmaak, het kleurenschema of de algemene stijl van de website. Aanpassingen aan het template worden uitsluitend centraal door of namens de stichting doorgevoerd.
4. Ter bescherming van de privacy en de digitale veiligheid van minderjarigen, is het niet toegestaan om foto's of video's van leerlingen op de openbare schoolwebsite te publiceren. Dit geldt ook indien er in het verleden algemene toestemming is gegeven. Voor het delen van

beeldmateriaal van leerlingen met de eigen achterban (ouders) dient uitsluitend gebruik te worden gemaakt van het beveiligde ouderportaal.

5. Het publiceren van beeldmateriaal van medewerkers (bijvoorbeeld op een 'teampagina') is slechts toegestaan indien de betreffende medewerker hiervoor expliciet schriftelijke toestemming heeft gegeven middels het daarvoor bestemde 'Toestemmingsformulier beeldmateriaal medewerkers'. Deze toestemming kan door de medewerker op elk moment worden ingetrokken, waarna de media onverwijld wordt verwijderd.
6. De directie van de school is verantwoordelijk voor de actualiteit van de informatie op de website en ziet erop toe dat de inhoud in overeenstemming is met dit reglement en de AVG-richtlijnen van Stichting PrimAH.

Artikel 14 – Instant messaging (IM)

Voor het gebruik van IM-diensten (Instant Messaging-diensten zoals WhatsApp, Messenger, Telegram, etc.) gelden onderstaande afspraken:

1. Het gebruik van IM-diensten voor werkgerelateerde doeleinden is uitsluitend toegestaan voor de communicatie tussen collega's onderling (medewerkers van Stichting PrimAH).
2. Bij het gebruik van IM-diensten tussen collega's dienen de volgende regels in acht te worden genomen:
 - a. Geen privacygevoelige informatie: Deel nooit persoonsgegevens van leerlingen, medische informatie, voortgangsrapportages of andere vertrouwelijke documentatie via IM-diensten. Gebruik hiervoor de daarvoor bestemde beveiligde systemen (zoals het leerlingvolgsysteem of de beveiligde mail).
 - b. Professioneel gebruik: Groepsapps tussen collega's zijn bedoeld voor praktische afstemming en informele professionele communicatie. Houd ook hier de fatsoensnormen in acht.
3. Voor het contact met externen gelden de volgende strikte verbodsbepalingen:
 - a. Geen contact met ouders/verzorgers: Het is medewerkers niet toegestaan om via IM-diensten te communiceren met ouders, voogden of verzorgers over schoolgerelateerde zaken. Hiervoor wordt uitsluitend gebruikgemaakt van de officiële communicatiekanalen van de school (zoals het ouderportaal of de zakelijke e-mail).
 - b. Geen contact met leerlingen: Direct contact tussen medewerkers en leerlingen via IM-diensten is niet toegestaan. Dit dient ter bescherming van de professionele distantie en de privacy van zowel de leerling als de medewerker.
 - c. Uitzonderingen: Alleen in acute noodsituaties of bij specifieke door het bestuur goedgekeurde activiteiten (zoals een schoolkamp waarbij snelle bereikbaarheid van

begeleiding noodzakelijk is) kan tijdelijk worden afgeweken van deze regel, mits de privacy gewaarborgd blijft.

4. Het gebruik van IM-diensten op privé-apparaten geschiedt op eigen risico. Medewerkers worden aangemoedigd om kritisch om te gaan met de instellingen en beveiliging van de apps en het apparaat. Zie voorwaarden artikel 7 van dit document.

Artikel 15 – Vertrouwelijke informatie

1. Het is verboden om zonder toestemming vertrouwelijke informatie aan derden te geven, via welk kanaal of gegevensdrager dan ook. Overtreding kan leiden tot (disciplinaire) maatregelen.
2. Werk je op een andere plek dan je vaste werkplek, dan gelden de regels en voorwaarden zoals beschreven in artikel 8 van dit document.
3. Zie je (mogelijk) een overtreding van deze regels? Meld dit direct bij de leidinggevende van de betrokken medewerker.
4. Voor niet-vertrouwelijke bestanden is er per afdeling een algemene plek op het netwerk om bestanden te delen. Vertrouwelijke informatie mag je daar **niet** uitwisselen. Het intern delen van vertrouwelijke informatie mag alleen via de daarvoor aangewezen locaties op het netwerk. Het extern delen van informatie gebeurt **altijd** met e-mailbeveiligingssoftware.
5. Het vermoeden hebben van of het lekken van vertrouwelijke informatie – al dan niet onbedoeld – dient meteen gemeld te worden bij de schoolleiding en/of Functionaris Gegevensbescherming/ Privacy Officer. Hiervoor geldt een termijn van maximaal 24 uur.

Artikel 16 – Controle

1. Controle vindt alleen plaats voor de doelen genoemd in artikel 3.2.

Deze controle is beperkt in omvang en wijze:

- a. Voor begeleiding/individuele beoordeling kan steekproefsgewijs zakelijke e-mail en/of post en zakelijk telefoonverkeer worden gecontroleerd indien er een gerechtvaardigd vermoeden is. Gesprekken kunnen worden opgenomen, zoals vooraf met jou is afgesproken.
- b. Conform bedrijfsregels kunnen jij en/of een aangewezen functionaris kopieën maken van zakelijke e-mail/post en opnames van zakelijke telefoongesprekken, voor bewijs/archivering.
- c. Voor virus- en beveiligingsdoeleinden kan e-mail en internetgebruik geautomatiseerd worden gecontroleerd.
- d. Om uitlekken van organisatiegeheimen/vertrouwelijke info te voorkomen kan steekproefsgewijs inhoudsfiltering plaatsvinden, of gericht als filteren niet kan en er een gerechtvaardigd vermoeden is. Verdachte e-mails worden apart onderzocht.
- e. Om negatieve publiciteit te voorkomen kan inhoudsfiltering plaatsvinden; verdachte berichten worden automatisch teruggestuurd en “verboden” sites geblokkeerd. Indien

- er een gerechtvaardigd vermoeden is, kan gericht post, en telefoonverkeer worden gecontroleerd.
- f. Voor het tegengaan van seksuele intimidatie of ander ongeoorloofd gedrag kan geautomatiseerde controle plaatsvinden; verdachte berichten worden automatisch teruggestuurd.
 - g. Voor het tegengaan van verboden gebruik gebeurt controle in principe geanonimiseerd en steekproefsgewijs.
 - h. Voor kosten- en capaciteitsbeheersing beperken we controle tot verkeersgegevens (tijd, hoeveelheid, omvang, etc.).
 - i. Stichting PrimAH mag sociale mediagebruik controleren, mits je daar vooraf over bent geïnformeerd. Controle is alleen toegestaan voor: begeleiding/individuele beoordeling, systeem- en netwerkbeveiliging, bescherming van bedrijfsgeheimen, voorkomen van negatieve publiciteit, tegengaan van seksuele intimidatie, naleving van afspraken over verboden gebruik, en kosten-/capaciteitsbesparing.
- 2. Controle gebeurt in beginsel op geaggregeerd niveau (niet herleidbaar tot personen). Bij een redelijke verdenking tegen een medewerker (of groep) kan gedurende een korte, vastgestelde periode gericht worden gecontroleerd.
 - 3. We beperken ons in principe tot verkeersgegevens. Alleen om zwaarwegende redenen controleren we inhoud.
 - 4. Bij geconstateerde overtredingen spreekt de leidinggevende de medewerker zo snel mogelijk aan en volgt een gesprek.
 - 5. Bij strafbaar internetgebruik kan Stichting PrimAH aangifte doen.
 - 6. E-mails, telefoongesprekken en post van (G)MR-leden en andere vertrouwensfunctionarissen zijn in beginsel uitgesloten van controle, behalve voor de veiligheid van het berichtenverkeer.
 - 7. De werkgever mag gegevens over het gebruik analyseren bij redelijke verdenking van ongeoorloofd gedrag, als andere middelen zijn uitgeput, er een zwaarwegend belang is en we rekening houden met de gevolgen en privacy. Gegevens worden bewaard zolang nodig is voor onderzoek en eventuele maatregelen.

Artikel 17 – Rechten van betrokkenen

- 1. Bij indiensttreding worden medewerkers geïnformeerd over dit reglement, de doelen, de aard van de gegevens, de herkomst en de inhoud van dit reglement (art. 33 Wbp).
- 2. Je kunt Stichting PrimAH vragen om een volledig overzicht van je verwerkte persoonsgegevens; je krijgt binnen 4 weken antwoord (art. 35 Wbp).
- 3. Je kunt verzoeken om correctie, aanvulling, verwijdering of afscherming als gegevens feitelijk onjuist, onvolledig voor het doel, niet ter zake dienend of onrechtmatig verwerkt zijn; binnen 4 weken volgt reactie (art. 36 Wbp).
- 4. Je kunt bezwaar maken tegen verwerking i.v.m. bijzondere persoonlijke omstandigheden; binnen 4 weken beoordeelt Stichting PrimAH of dit gerechtvaardigd is en stopt zo nodig de verwerking (art. 40 Wbp).

Artikel 18 – Klachten

Vind je dat je rechten door dit reglement zijn geschaad? Meld dit bij Stichting PrimAH. Je klacht wordt zo snel als redelijkerwijs kan, vertrouwelijk behandeld.

Artikel 19 – Slotbepalingen

1. Dit reglement laat rechten/bevoegdheden uit wet, CAO of andere regelingen voor Ondernemingsraad, (G)MR en/of Stichting PrimAH onverlet.
2. Stichting PrimAH en de Gemeenschappelijke Medezeggenschapsraad (GMR) kunnen dit reglement in overleg wijzigen/aanpassen. Wijzigingen worden schriftelijk vastgelegd, ondertekend en bekendgemaakt aan medewerkers.
3. In onvoorziene omstandigheden mag Stichting PrimAH afwijken als er een direct en zwaarwegend belang is. De voorzitter van de GMR wordt direct geïnformeerd.
4. Het reglement is geldig vanaf akkoordverklaring en wordt daarna stilzwijgend met één jaar verlengd, tenzij Stichting PrimAH of de GMR minimaal één maand vóór het einde van de jaartermijn schriftelijk een wijziging of beëindiging aankondigt.
5. Als wetgeving of maatschappelijke ontwikkelingen daartoe aanleiding geven, overleggen Stichting PrimAH en de GMR over eventuele aanpassingen.

Artikel 20 – Algemeen

Onvoorziene situaties

In gevallen waarin dit reglement niet voorziet, beslist Stichting PrimAH naar redelijkheid, in lijn met de strekking van dit reglement.

Inwerkingtreding

Dit reglement is goedgekeurd op 29-09-2026 en treedt in werking op 1 november 2026. Alle eerdere regelingen, gebruiken en afspraken vervallen per die datum.