Protocol internet-, e-mail- en social media gebruik

Achtergrond

De gemeente Huizen communiceert met haar inwoners ook via digitale kanalen zoals e-mail en social media. Daarnaast is internet een belangrijk middel voor medewerkers voor de uitoefening van hun functie. De gemeente Huizen verlangt van medewerkers dat zij digitaal vaardig zijn en de hiervoor beschikbaar gestelde faciliteiten optimaal gebruiken. Indien dergelijke faciliteiten niet op de juiste wijze worden gebruikt kan dit leiden tot fraude en/of schending van de privacy van inwoners en imago-schade van de gemeente Huizen.

Doelstelling

Dit protocol geeft de gedragsregels weer voor het internet-, e-mail- en social media gebruik binnen de gemeente Huizen. Het protocol biedt richtlijnen en handvatten om tot een juiste balans te komen tussen verantwoord gebruik van internet, e-mail en social media en de bescherming van privacy van inwoners, bedrijven en medewerkers.

Gebruikersaccount

Voor gebruik van deze faciliteiten geldt dat medewerkers vanaf de start van hun werkzaamheden voor de gemeente Huizen een persoonlijk zakelijk gebruikersaccount ontvangen (voor gebruik van internet en e-mail). Bij vertrek van medewerkers, door uitdiensttreding of beëindiging van de werkzaamheden, wordt het gebruikersaccount eerst geblokkeerd. Daarna wordt tot maximaal 1 maand nadien in een automatisch gegenereerd antwoordbericht in het e-mail account aangegeven dat de betreffende medewerker niet langer werkzaamheden voor de gemeente Huizen verricht. Vervolgens wordt het gebruikersaccount verwijderd samen met alle e-mailberichten in de postbus.

Reikwijdte

Dit protocol is bedoeld voor alle interne en externe medewerkers van de gemeente Huizen, inclusief het college van burgemeester en wethouders van de gemeente Huizen. Het protocol is met name van toepassing op het zakelijke gebruik van internet, e-mail en social media. Iedere medewerker moet zich bewust zijn van eventuele gevolgen van privégebruik van deze kanalen voor de gemeente Huizen.
In dit protocol zijn ook regels vastgelegd voor het controleren van verantwoord gebruik van de genoemde faciliteiten. Dit is ter beveiliging van het computernetwerk en het voorkomen van onrechtmatig gebruik van deze faciliteiten.
Dit protocol is opgesteld in samenwerking met de Ondernemingsraad (OR).

Protocol

Hieronder volgt het protocol artikelsgewijs.

Hoofdstuk 1. Internet

Artikel 1. Algemene uitgangspunten

1. Het opslaan, distribueren, bewerken, verzenden, downloaden of reproduceren van software en informatie of ander materiaal dat onder bescherming van de auteursrechten valt, is niet toegestaan zonder toestemming van de rechthebbende.
2. Het is niet toegestaan 'executable files' (uitvoerbare bestanden, bijvoorbeeld met de extensie .exe) vanaf het internet te openen of op te slaan. Als dit toch noodzakelijk is voor de uitvoering van een taak moet dit worden afgestemd met een medewerker van het team Informatisering en automatisering (I&A).

Artikel 2. Internetgebruik

1. Internet is bedoeld voor functioneel, zakelijk gebruik door medewerkers. Gebruik voor privédoeleinden is toegestaan, als dit de voortgang van werkzaamheden en/of het functioneren van de medewerker niet nadelig beïnvloedt.
2. Het is niet toegestaan het netwerk zodanig te belasten dat daardoor vertragingen op het netwerk ontstaan. Als dit toch noodzakelijk is voor de uitvoering van werkzaamheden moet dit worden afgestemd met een medewerker van het team I&A.
3. Het internet gebruiken voor het posten, verzenden, reproduceren en downloaden van bedreigende, obscene, seksistische, racistische of anderszins moreel verwerpelijke inhoud is niet toegestaan.
4. Het internet gebruiken voor het bewust bezoeken van websites met bedreigende, obscene, seksistische, racistische of anderszins moreel verwerpelijke inhoud is niet toegestaan.
5. Het is niet toegestaan het internet te gebruiken voor met de wet strijdige activiteiten.

Hoofdstuk 2. E-mail

Artikel 3. Algemene uitgangspunten

1. De gemeente Huizen onderscheidt twee soorten e-mailberichten:
   -formele berichten die worden opgeslagen in het Document Management Systeem (DMS) en
   -berichten, meestal informeel van inhoud, die niet hoeven te worden opgeslagen.
2. Elektronische aanvragen worden alléén in behandeling genomen als deze zijn verstuurd via daarvoor bestemde webformulieren op de gemeentelijke website. Zijn deze op een andere wijze verstuurd (zoals bijvoorbeeld per e-mailbericht), dan wijst de ontvanger de afzender op de juiste kanalen.
3. E-mailberichten met in het onderwerp het woord "vertrouwelijk" (of aanduidingen zoals persoonlijk, privé of dergelijke) mogen alleen door de afzender en de beoogde ontvanger worden ingezien. Dit geldt ook voor alle e-mailberichten verzameld in een map met een naam die deze vertrouwelijkheid aangeeft.
4. Wanneer een bijlage van een e-mailbericht ondanks het toepassen van alle beschikbare hulpmiddelen niet kan worden geopend, nemen we het bericht niet in behandeling.
   De ontvanger informeert de afzender hierover.
5. Bij een gebrekkig of onvolledig e-mailbericht verzoeken we de afzender om de e-mail binnen een gestelde termijn met de nodige gegevens aan te vullen. Als hierop geen antwoord komt, is de gemeente gerechtigd het bericht niet in behandeling te nemen.
6. Een e-mailbericht met een verzoek om informatie als bedoeld in artikel 3 van de Wet openbaarheid van bestuur wordt niet in behandeling genomen. De afzender wordt hierover geïnformeerd en wordt naar de juiste kanalen verwezen.

Artikel 4. E-mail ontvangen

1. Iedere medewerker controleert, minimaal eens per werkdag, zijn of haar e-mailpostbus.
2. Wees terughoudend bij het openen van e-mailberichten en verwijder e-mailberichten die niet betrouwbaar lijken direct. Dit bevordert de informatieveiligheid.
3. Sla formele/belangrijke berichten altijd op in het Document Management Systeem (DMS).
4. Iedere medewerker controleert wekelijks zijn of haar spampostbus. Zo wordt voorkomen dat e-mailberichten, die onterecht als spam zijn aangemerkt, worden gemist.
5. Iedere medewerker schoont regelmatig zijn of haar postbus en de onderliggende mappen. Zo worden e-mailberichten niet langer bewaard dan nodig is en wordt de capaciteit van het systeem niet onevenredig belast (maximum 5 Gigabyte per gebruiker).
6. Voor de afhandeling van e-mailberichten gelden servicenormen. Deze zijn te vinden op onze website.

7. Stel een afwezigheidsregel in bij een geplande afwezigheid van langer dan 2 werkdagen. Zie hiervoor de handleiding op het intranet in de groep Automatisering ("Regels instellen in Outlook").
8. Zorg er voor dat meerdere collega's zijn gemachtigd om je e-mailbox in te zien. Zo kunnen in jouw e-mailbox binnenkomende e-mailberichten tijdens ziekte of andere afwezigheid toch worden afgehandeld.
9. De beheerders van algemene postbussen (bijvoorbeeld facturen of inkoop) zorgen, voor zover nodig, voor de registratie en eventuele doorzending van e-mailberichten.
10. Iedere medewerker die een e-mailbericht ontvangt dat dreigend, seksueel getint, intimiderend of racistisch is, meldt dit aan de leidinggevende.
11. Indien een e-mailbericht verkeerd is geadresseerd wordt de afzender hiervan op de hoogte gesteld.

Artikel 5. E-mail verzenden

1. Gebruik e-mail voor interactieve berichten waarop een reactie wordt verwacht, of voor berichten met een zekere urgentie. Gebruik voor informatieve berichtgeving aan een groep medewerkers of aan alle medewerkers het intranet.
2. Houdt zakelijke en privé e-mailberichten uit elkaar. Gebruik het zakelijke e-mailadres alleen voor e-mailberichten die uit hoofde van de functie worden verzonden.
3. Ga zorgvuldig om met het verzenden van persoons- en vertrouwelijke gegevens. Zowel intern als extern gerichte e-mailberichten met dit type informatie wordt verstuurd met de aanduiding "vertrouwelijk" in het onderwerp. Extern gerichte e-mailberichten worden in dit geval altijd versleuteld verstuurd, via de "beveiligde e-mail" optie.
4. Bij communicatie per e-mail worden dezelfde regels in acht genomen als in het dagelijkse intermenselijke verkeer. Het verzenden van dreigende, seksueel getinte, intimiderende, racistische of anderszins niet integere berichten is niet toegestaan.
5. E-mailberichten worden zo gericht mogelijk, alleen aan diegenen die rechtstreeks betrokken zijn, verstuurd. Van verzendlijsten wordt beperkt en weloverwogen gebruik gemaakt.
   Gebruik de Bcc-optie in verzendlijsten. Hiermee wordt voorkomen dat de ontvanger een antwoord aan iedereen stuurt wanneer deze per ongeluk de knop 'Allen beantwoorden' gebruikt.
6. Gebruik de Cc-optie voor ontvangers die geen actie hoeven te ondernemen.
7. Houd rekening met de ontvanger voor wat betreft de bijlagen. Beperk de grootte van de bijlagen (voor het gehele bericht maximaal 10 MB) en stuur de bijlagen in een algemeen leesbaar en bruikbaar formaat. Biedt bijlagen bij voorkeur aan in een formaat dat geldt als een zogenaamde open standaard, zoals PDF en ODF (.odt)*. Neem voor het verzenden van grotere of afwijkende bijlagen vooraf contact op met een medewerker van de helpdesk automatisering van het team Informatisering en Automatisering (I&A).
8. Gebruik van clouddiensten, zoals dropbox, google drive, one drive en we transfer, voor het verzenden van grote bestanden is niet toegestaan. Deze cloud-diensten zijn niet geschikt voor het uitwisselen van zakelijke informatie. Er is geen controle op de gegevensoverdracht: welke documenten worden vrijgegeven, waar zij worden opgeslagen, aan wie zij worden verstrekt en op welk moment. Hierdoor wordt het risico op datalekken ontoelaatbaar vergroot en zijn er nagenoeg geen mogelijkheden om de gevolgschade te beperken of te herstellen.
9. Elk uitgaand e-mailbericht wordt voorzien van een handtekening. Zie hiervoor de aanwijzingen op het intranet ("Handtekening toevoegen in Outlook" in de groep Automatisering).

Hoofdstuk 3. Social media

Artikel 6. Algemene uitgangspunten

1. Vanuit de verschillende mediakanalen formuleren we, conform de in teamverband gemaakte werkafspraken , een eenduidig antwoord naar het publiek: via elk kanaal hetzelfde antwoord.
2. In berichtgeving wordt begrijpelijke en feitelijke informatie gebruikt.
3. Berichten zijn qua toon vriendelijk en dienstverlenend.
4. Het gebruik van Whatsapp en Whatsapp-groepen in het contact tussen medewerkers en met inwoners wordt door de gemeente Huizen gestimuleerd en aangemoedigd.
5. Het is niet toegestaan om vertrouwelijke (gemeentelijke) gegevens via Whatsapp te delen omdat dit niet veilig is. Het delen van persoonsgegevens van inwoners via diensten als Whatsapp is onder Europese wet- en regelgeving verboden.

Artikel 7. Gebruik van social media

Zakelijk gebruik van social media

1. Berichtgeving die online staat, kan niet zomaar verwijderd of gewijzigd worden. Bij de afweging om inhoud te plaatsen houden we hiermee rekening. Als de gemeente onjuiste berichtgeving tegenkomt wordt er gekeken naar een eventuele rectificatie .
2. Bij het plaatsen van materiaal wordt het wettelijk vastgelegde beeld-, auteurs- en citaatrecht in acht genomen.
3. (Bijzondere) persoonsgegevens of vertrouwelijke informatie delen we nooit via social media.
4. Bij communicatie via social media worden dezelfde regels in acht genomen als in het dagelijkse intermenselijke verkeer. Het verzenden van dreigende, seksueel getinte, intimiderende, racistische of anderszins niet integere berichten is niet toegestaan.
5. Bij het plaatsen van inhoud verwachten we zorgvuldigheid: spel-, stijl- of schrijffouten worden voorkomen.
6. Voor de afhandeling van berichten gelden richtlijnen. Vragen die binnenkomen via social media worden binnen 24 uur beantwoord. Laat het antwoord langer op zich wachten? Dan laten we dit aan de vraagsteller weten.

Privégebruik van social media

7. We hanteren een duidelijk onderscheid tussen privé en zakelijk gebruik van social media. Op persoonlijke titel wordt geen inhoud geplaatst die gerelateerd is aan de werksituatie.
8. Het privégebruik van social media is toegestaan, als dit de voortgang van werkzaamheden en/of het functioneren van de medewerker niet nadelig beïnvloedt.

Artikel 8. Berichten die niet in behandeling worden genomen

1. Aanvragen die via social media worden ingediend, worden niet in behandeling genomen. Hierbij wordt verwezen naar de juiste kanalen voor de desbetreffende aanvraag.
   Een uitzondering is de MOR-melding: de melding wordt doorgezet naar de betreffende afdeling, tegelijkertijd wijzen we de afzender op gebruik van het juiste kanaal.
2. We geven geen antwoord op persoonlijke statusvragen, hierbij verwijzen we naar de juiste kanalen.
3. We reageren in principe niet op uitingen, waarin wordt gescholden of waarin beledigend, opruiend of kwetsend taalgebruik wordt gebezigd.
4. In overleg met de directie kan hiervan worden afgeweken.

Hoofdstuk 4. Controle, onderzoek en sancties internet, e-mail en social media

Artikel 9. Rechten werkgever

1. De directie is bevoegd het gebruik van e-mail, internet en social media steekproefsgewijs en onder voorwaarden te controleren met het oog op legitieme doelstellingen zoals:
    a. Het beheersen van de kosten en capaciteit inzake e-mail- en internetgebruik;
    b. het voorkomen van de verspreiding van schadelijke berichten;
    c. het waarborgen van de vertrouwelijkheid van informatie;
    d. het voorkomen van overtreding van wet- en regelgeving en
    e. de concrete verdenking van misbruik door een werknemer.

2. De werkgever registreert en controleert geen gebruiksgegevens (zoals bezochte websites en tijdsbesteding) over het internetgebruik van medewerkers.
   Ook wordt de inhoud van e-mailberichten niet gecontroleerd. In geval van zwaarwegende redenen kan hiervan worden afgeweken. In dit geval wordt hiervoor van te voren toestemming gevraagd aan de Ondernemingsraad (OR) en wordt hiervan een melding gedaan bij de Autoriteit Persoonsgegevens (AP).
3. Voor de heimelijke controle van medewerkers geldt, naast de in artikel 9 onder lid 1 genoemde voorwaarden, dat bij de AP een voorafgaand onderzoek wordt aangevraagd.
   De werkgever mag pas met het onderzoek beginnen wanneer de AP dit heeft goedgekeurd.
4. De werkgever informeert de betrokken medewerkers achteraf altijd over de heimelijke controle, ongeacht de uitkomst van het onderzoek.
5. De werkgever kan filters gebruiken om de toegang tot bepaalde websites te verhinderen.

Artikel 10. Rechten medewerkers

1. Een medewerker heeft het recht de in het kader van de controles als bedoeld in artikel 9 geregistreerde gegevens over hem of haar in te zien.
2. Een medewerker ontvangt op zijn of haar verzoek binnen twee weken een kopie van gegevens die over hem/haar zijn geregistreerd. Het verzoek om inzage wordt ingediend bij de directie.
3. Een medewerker kan de directie verzoeken om feitelijk onjuiste of onvolledige gegevens uit de registratie te verbeteren, aan te vullen of te verwijderen.
4. De directie beslist binnen twee weken op de onder lid 2 en 3, genoemde verzoeken. Eventuele correcties, aanvullingen of verwijderingen van gegevens worden direct uitgevoerd.

Artikel 11. Sancties

1. Bij de overtreding van dit protocol door de medewerker kan de werkgever een disciplinaire maatregel opleggen zoals beschreven in artikel 16 van de CAR/UWO.
2. De werkgever kan bij overtreding van dit protocol bepalen dat de medewerker geen toegang meer heeft tot het e-mailsysteem en het internet.
3. Voor dat tot een maatregel zoals bedoeld, onder lid 1 en 2, wordt besloten, ontvangt de medewerker een schriftelijke waarschuwing waarin hij of zij wordt gesommeerd de overtredingen te staken.
4. Van artikel lid 3 kan worden afgeweken wanneer de aard en/of omvang van de overtreding aanleiding geeft tot het direct opleggen van een disciplinaire maatregel zoals beschreven in artikel 16 van de CAR/UWO.

Hoofdstuk 5. Overige bepalingen.

Artikel 12. Inwerkingtreding en citeertitel

1. Dit protocol is op 25 januari 2018 vastgesteld door het college van de gemeente Huizen na instemming door de OR.
2. Dit reglement wordt aangehaald als "Protocol internet, e-mail en sociale media gebruik".

Bijlage 1: Definities en verantwoordelijkheden

Artikel 1. Definities

1. E-mail: berichten die op elektronische wijze tussen computers worden uitgewisseld. Gemeentelijk e-mailadres: eindigend op @huizen.nl.
2. Formele berichten: berichten met een zekere proces ondersteunende waarde.
3. Social media: verzamelbegrip voor online platformen waar gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Denk hierbij aan Facebook, Instagram, LinkedIn, Twitter en Whatsapp. De gemeente heeft drie social media accounts: Facebook (facebook.com/gemeenteHuizen), Twitter (@gemeentehuizen) en LinkedIn.
4. Webformulieren: formulieren die online via huizen.nl kunnen worden ingediend.
5. Persoonsgegevens: elk gegeven over een identificeerbare of geïdentificeerde natuurlijke persoon. Deze informatie is of te herleiden naar, of gaat over, iemand. De Wet bescherming persoonsgegevens (Wbp) zorgt voor de wettelijke bescherming van deze gegevens.
   Per 25 mei 2018 vervalt de Wbp en wordt deze vervangen door de Algemene verordening gegevens-bescherming (AVG).
6. Vertrouwelijke informatie: Met vertrouwelijke informatie wordt alle informatie bedoeld die niet als zijnde 'openbaar' is geclassificeerd. Dit betekent dat deze informatie niet voor iedereen toegankelijk mag zijn.
   Bijvoorbeeld: informatie die slechts toegankelijk mag zijn voor medewerkers van de gemeente of ook informatie die slechts toegankelijk mag zijn voor een specifieke groep gebruikers of de direct geadresseerden.
7. ODF : open document format; de open standaard voor de digitale uitwisseling van documenten.
8. .ODT : open document tekst; dit is het bestandstype voor een tekstdocument in het ODF formaat.
9. PDF : portable document format.
10. BCC : blind carbon copy/blinde kopie. Niet zichtbaar is dat er een kopie van het e-mailbericht naar andere ontvangers is gestuurd.
11. Cc : carbon copy/kopie. Voor alle ontvangers is zichtbaar aan wie het e-mailbericht nog meer is gestuurd.
12. DMS : Document Management Systeem (op dit moment is dit Join van Decos).

Artikel 2. Verantwoordelijkheden

1. Iedere medewerker is verantwoordelijk voor de juiste afhandeling van berichtenverkeer volgens dit protocol.
2. Iedere medewerker is verantwoordelijk voor het acceptabele gebruik van ICT en social media volgens dit protocol.
3. Het afdelingshoofd Bestuur, burgerzaken en ondersteuning (BBO) is verantwoordelijk voor het opstellen en onderhouden van procedures aangaande het e-mailverkeer.
4. Het afdelingshoofd BBO is verantwoordelijk voor de actualiteit van dit protocol.