gemeente Brunssum

GEMEENTEBLAD

Officiële uitgave van de gemeente Brunssum

Nr. 39315

20 februari 2019

Beleidsregel van het college van burgemeester en wethouders van de gemeente Brunssum houdende regels omtrent communicatie Gemeentelijke richtlijnen voor het gebruik van internet, e-mail en sociale media

Het college van B&W heeft op 29 januari 2019 de 'Gemeentelijke richtlijnen voor het gebruik van internet, e-mail en sociale media' vastgesteld. Deze richtlijnen treden de dag na bekendmaking in werking. Tevens is besloten om de 'Gemeentelijke gedragscode voor e-mail en internet' en 'Richtlijnen voor het gebruik van social media gemeente Brunssum (2017)' in te trekken.
De oude 'Gemeentelijke gedragscode voor e-mail en internet' was gedateerd. Deze is dan ook geactualiseerd en daarnaast samengevoegd met de 'Richtlijnen voor het gebruik van social media gemeente Brunssum (2017)'. Deze onderwerpen zijn zo nauw aan elkaar gerelateerd dat dit een beter overzicht biedt voor de medewerkers. Zij hoeven nu niet meer op zoek naar twee documenten maar lezen alles wat ze moeten weten in deze nieuwe richtlijnen.
Deze beleidsregel maakt de rechten en plichten van ieder die werkzaam is bij of voor de gemeente Brunssum met betrekking tot internetgebruik expliciet. Deze regeling zorgt ervoor dat alle medewerkers bedachtzaam en binnen de gegeven kaders gebruikmaken van internet, e-mail en sociale media.

Samenvatting

Internet
- De internetvoorziening is bedoeld voor het opvragen en uitwisselen van werkgerelateerde informatie. De medewerker is zelf verantwoordelijk voor het juiste gebruik van deze voorziening.

E-mail
- Het e-mailverkeer dient betrouwbaar, duidelijk en juist te gebeuren. Persoonlijke en vertrouwelijke informatie moet beveiligd verzonden worden naar externen.
- De ambtenaar maakt gebruik van een standaardhandtekening en een afwezigheidsregel.
- De medewerker dient zijn postvak dagelijks te controleren. Daarnaast dient de medewerker zich te houden aan de registratieplicht en aan de vastgelegde behandelingstermijnen.

Sociale media
- Wie werkzaam is voor de gemeente Brunssum is dat ook buiten de werksfeer.
- De medewerker is in zijn hoedanigheid als ambtenaar niet aanwezig op sociale media. Bij gebruik van sociale media is het niet toegestaan om vanuit de eigen taak of functie werkgerelateerde informatie te communiceren.
- Blijf alert bij het mixen van privé en werk.

Beveiliging
- De medewerker dient zijn werkplek te beveiligingen door een veilig wachtwoord te gebruiken, het computerscherm te vergrendelen en het 'clean desk'-principe te hanteren.
- Wees alert met phishingmails, vreemde gegevensdragers en werk via een beveiligde verbinding.

Privacy
- De medewerker dient zich als verwerkingsverantwoordelijke aan de beveiligingseisen te houden. Verliest de medewerker onverhoopt toch potentieel privacygevoelige data (zowel analoog als digitaal), dan moet dit datalek zo snel mogelijk worden gemeld.
- De medewerker heeft recht op privacy en wordt niet actief gemonitord. Bij gerechtvaardigd belang kan het internetgebruik worden onderzocht.
- Bij onvoorziene, langdurige afwezigheid kan de werkgever de persoonlijke e-mailbox van de betreffende werknemer inzien.

Inleiding

Deze regeling is gebaseerd op “Nota integriteitbeleid” (2012) en is een opvolger van “Gemeentelijke gedragscode gebruik E-mail en Internet” (2008) en “Richtlijnen voor het gebruik van social media gemeente Brunssum” (2012). Dit document maakt het gewenste gebruik van internet, e-mail en sociale media duidelijk en bespreekt in het verlengde daarvan de verschillende facetten van beveiliging en privacy.
Alle medewerkers en externen die werkzaam zijn voor gemeente Brunssum en gebruikmaken van de e-mail- en internetvoorziening van de gemeente Brunssum worden op de hoogte gesteld van en zal zich dienen te conformeren aan deze regeling.
Integriteit bij de overheid heeft twee kanten, enerzijds in het omgaan met de eigendommen van de gemeente, anderzijds in het handelen met derden, zowel intern als extern (Nota integriteitbeleid 2012, p. 2). Hierbij gelden de kernwaarden zoals deze zijn geformuleerd in “Organisatieplan 2016”:

- Samenwerken: de ambtenaar doet het samen en is flexibel.
- Professionaliteit: de ambtenaar is transparant en klantgericht.
- Integriteit: de ambtenaar is betrouwbaar.
- Lef: de ambtenaar toont lef, passie en creativiteit in zijn werk.

1. Internet

In deze paragraaf wordt ingegaan op het algemene gebruik van internet.

1. Alle medewerkers van de gemeente Brunssum maken gebruik van een beveiligd netwerk. In de autorisatie is de toegang tot het internet als generieke functionaliteit. Het internet is in eerste instantie bedoeld om informatie te kunnen opvragen en uitwisselen. Deze voorziening is gecreëerd om werkgerelateerde informatie op te vragen en uit te wisselen. Beperkt privé gebruik van het internet is toegestaan.
2. Het is niet toegestaan sites te bezoeken die aanstootgevend materiaal bevatten.
3. Het is niet toegestaan software te downloaden of te uploaden. Aan applicatiebeheerders is het toegestaan software te downloaden voor zover het zakelijk gebruik betreft.
4. Iedere medewerker is zelf verantwoordelijk voor een juist gebruik van de internetvoorziening. Het afdelingshoofd is binnen zijn/haar organisatieonderdeel verantwoordelijk voor het juiste gebruik van internet conform deze regeling.

2. E-mail

De gemeente Brunssum beschikt over drie soorten e-mailadressen. Het betreft de e-mailadressen van gedeelde mailboxen, zoals het algemene e-mailadres (gemeente@brunssum.nl), distributielijsten (iedereen in deze lijst ontvangt de e-mail in zijn persoonlijke mailbox) en de individuele e-mailadressen (bijvoorbeeld: anton.van.bronsheim@brunssum.nl). Het algemene e-mailadres is bedoeld voor externe communicatie, zoals posters, brieven en berichten. Het beheer van deze postbus is een verantwoordelijkheid van de afdeling Informatiemanagement.
De individuele e-mailadressen zijn bedoeld voor het formele contact dat ambtenaren hebben met burgers, instanties, collega's, etc. Dit adres kan door de individuele medewerker worden doorgegeven aan relaties/contacten alsmede vermeld worden op visitekaartjes.
Binnen deze paragraaf zullen we dieper ingaan op het gebruik van e-mailberichten en de e-mailbox. Eerst zal de communicatie met externen worden behandeld, daarna de interne communicatie.

2.1 Extern

De e-mailgedragslijn voor overheden geldt als volgt: ‘altijd antwoord, tijdig antwoord’. Eenvoudige vragen dienen binnen 2 werkdagen van een antwoord te worden voorzien. Deze hebben betrekking op bekende feiten of procedures, zoals openingstijden, parkeerregels, vergunningprocedures, en dergelijke. Voor complexe vragen geldt een langere termijn, waarbij de burger in ieder geval binnen 10 werkdagen geïnformeerd dient te zijn over de verwachte behandelingstermijn. Dit is de verantwoordelijkheid van de desbetreffende afdeling (zie ook ontvangstbevestiging). Indien deze behandelingstermijn niet kan worden nagekomen, dient de afzender op de hoogte te worden gesteld van de nieuwe termijn. Deze gedragslijn is in te zien op overheid.nl: “E-mailgedragslijn voor overheden”.

Alle e-mailberichten worden gezien als post van de gemeente Brunssum. Bij het gebruik van e-mail voor de externe communicatie is het van belang de onderstaande aandachtspunten te volgen. Houd

er altijd rekening mee dat communicatie met externen volgens de AVG-wetgeving plaatsvindt (voor meer informatie, zie paragraaf "Privacy").

Aandachtspunten bij het verzenden van uitgaande e-mailberichten (extern)

1. E-mail behoort tot de officiële kanalen om formele post te versturen. (Dit geldt niet slechts voor schriftelijke post).
2. Te versturen e-mailberichten dienen steeds duidelijk van een onderwerp voorzien te worden. Houd het onderwerp kort maar krachtig door maximaal drie woorden te gebruiken.
3. Verder dient onder aan het bericht steeds een duidelijke afzender vermeld te worden (voor sjabloon zie "Instructie instellen standaardhandtekening Outlook"). De medewerker moet hierbij gebruikmaken van de handtekening die hij/zij in de Outlook-mail kan toevoegen zodat deze automatisch in elke te verzenden e-mail staat. Op Intranet kan de medewerker een handleiding vinden waarin staat hoe dit moet. Daarin staat ook het verplichte sjabloon voor de standaardhandtekening die gehanteerd wordt bij gemeente Brunssum.
4. Te versturen berichten dienen kort en duidelijk te zijn en moeten een functioneel karakter hebben. Daarnaast dient de inhoud van de e-mailberichten betrouwbaar en juist te zijn.
5. Er dient selectief omgegaan te worden met het versturen van kopieën naar anderen (de CC-functie).
6. Werk altijd volgens de AVG-wetgeving als er persoonsgegevens mee gemoeid gaan. Bij het verzenden van een e-mail met persoonsgegevens dient de medewerker gebruik te maken van de optie beveiligd mailen in Outlook. Vanuit het zaaksysteem kan de medewerker een zaak als bijlage versturen en zo de e-mail beveiligd verzenden.
7. De AVG geeft mensen onder andere het recht op inzage en het recht op vergetelheid. De burger heeft het recht om de persoonsgegevens die de gemeente van hen verwerkt in te zien. Deze inzage moet dan ook gegeven kunnen worden. Dit geldt ook voor Outlook: de persoonsgegevens die in Outlook staan, dienen verwijderd te worden wanneer een burger daarom verzoekt.
8. Het is niet toegestaan dreigende, discriminerende, seksueel getinte dan wel racistische berichten te versturen naar externen (zowel als internen). De inhoud voldoet in ieder geval aan dat wat is opgenomen in de "Nota integriteitbeleid" (2012).

Aandachtspunten bij het ontvangen van inkomende externe e-mailberichten

1. De individuele e-mailbox dient door de daarvoor verantwoordelijke medewerker regelmatig (minimaal eenmaal per dag) op inkomende e-mailberichten gecontroleerd en behandeld te worden. DIV (documentaire informatievoorziening) controleert de algemene e-mailbox (gemeente@brunssum.nl) meerdere keren per dag. E-mailberichten die binnenkomen op gemeente@brunssum.nl en die als informeel zijn aan te merken, worden na opening direct doorgestuurd (voor zover van toepassing) aan de betreffende ambtenaar. De als formeel aan te merken berichten worden geregistreerd. De zaken worden voorzien van een afhandelingsprocedure, waarna ze (voor zover van toepassing) worden doorgestuurd aan de betreffende afdeling. Deze stelt de betrokkene op de hoogte van de procesduur en neemt de verdere afhandeling voor zijn rekening.
2. Het is de verantwoordelijkheid van de individuele medewerker om inkomende e-mailberichten (op het persoonlijke e-mailadres) die een formeel karakter dragen direct door te sturen naar het algemene e-mailadres van de gemeente. DIV waarborgt de formele registratie en verstuurt iedereen een ontvangstbevestiging, tenzij hier andere afspraken aan ten grondslag liggen. De verdere afhandelingsprocedure van het bericht zal daarbij door de afdeling Informatiemanagement worden ingebracht in het documentmanagementsysteem, waarna vervolgens de inhoudelijke afhandeling door de betreffende ambtenaar zal dienen te geschieden.
3. Te registreren e-mail dient opgeslagen te worden in het zaaksysteem (Verseon). Voor iedere medewerker geldt het recht en de plicht om informatie te archiveren/bewaren. Redenen om informatie te registreren zijn: bewijs (dat het document ook echt bestaat), beheersing (de afhandeling wordt bewaakt), vindplaats (het document is terug te vinden) en overzicht (het genereren van managementinformatie). Informatie dient gestructureerd en te allen tijde voor betrokkenen toegankelijk te zijn.
4. Indien een medewerker afwezig is, bijvoorbeeld tijdens zijn vakantie, dient hij er zelf voor te zorgen dat aan hem geadresseerde e-mails worden behandeld. Activeer in het geval van afwezigheid de afwezigheidsregel (zie hiervoor de handleiding "[Outlook 2016] Instructie automatisch antwoorden bij afwezigheid/vakantieregel instellen"). In deze afwezigheidsregel geeft de medewerker aan wanneer hij/zij weer aanwezig is en wie het vervangend contactpersoon is. Zo is de verzender op de hoogte. Deze afwezigheidsregel dient formeel en zowel intern als extern van toepassing te zijn.
5. Langdurige afwezigheid kan voorkomen bij het einde van het dienstverband en pensionering van de medewerker (te voorzien door diens leidinggevende), maar ook bij langdurige ziekte waarbij de medewerker zelf niet in staat is om van huis uit enige actie te ondernemen of wegens het overlijden van een collega. Zulk soort gevallen zijn niet vooraf te voorzien door de leidinggevende en kunnen ertoe leiden dat de werkgever (leidinggevende, directe (ex-)collega's of een benoemd

intern vertrouwenspersoon) in de persoonlijke e-mailbox van een medewerker zal kijken. (Zie ook 'eigen privacy'.) Bij langdurige aanwezigheid waarbij de medewerker wel zelf in staat is vanuit thuis actie te ondernemen, bestaat er de mogelijkheid om collega's te machtigen voor het gebruik van de persoonlijke e-mailbox. Dit kan de medewerker geheel zelfstandig en op basis van eigen toestemming instellen (de handleiding is te vinden op Intranet). Hierbij dient de medewerker ook een afwezigheidsregel in te stellen. Bij gevallen die te voorzien zijn is het de verantwoordelijkheid van de medewerker om zaken over te dragen dan wel te registeren. De persoonlijke e-mailbox wordt hierbij in principe niet opengesteld.

6. Binnenkomende e-mailberichten die verdacht lijken dienen niet geopend te worden. Men dient direct contact op te nemen met de functionaris informatiebeveiliging of met een medewerker van de afdeling Informatiemanagement. Voor meer informatie zie paragraaf 'Beveiliging'.

2.2 Intern

1. Er dienen niet meer berichten verstuurd te worden dan strikt noodzakelijk, dit om irritatie en vervuiling tegen te gaan. Het betreft hier met name het ondoelmatig gebruik van de functie "Alle Medewerkers Brunssum" (i.c. collegeleden en alle medewerkers werkzaam binnen de ambtelijke organisatie). Er dient bij het versturen van e-mailberichten aan alle medewerkers een relatie tot het werk aanwezig te zijn.
2. De te versturen berichten dienen betrouwbaar, juist, kort en volledig te zijn. Ook het onderwerp van het e-mailbericht moet kort en helder zijn.
3. Iedere medewerker dient bij aanwezigheid dagelijks zijn/haar postbus te controleren op ingekomen berichten.

3. Sociale media en privé internetgebruik

Sociale media zijn media die gebruikmaken van online-technologieën om sociale interactie te bevorderen. Door gebruikers zelf content te laten produceren in plaats van alleen te consumeren, veranderen sociale media de traditionele informatieverspreiding in sociale media-dialogen. Ze dragen op die manier bij aan democratisering van kennis en informatie. Voorbeelden van sociale media zijn Facebook, Twitter, Instagram, blogs, Youtube, Linkedin etc.
Privé- en werk-gerelateerd zijn niet altijd gemakkelijk te scheiden op sociale media. Dit document biedt houvast om met vertrouwen actief online te participeren. Daarvoor zijn regels en richtlijnen opgesteld voor het gebruik van sociale media, zowel binnen de ambtelijke organisatie als daarbuiten.
Dit document heeft alleen betrekking op de ambtelijke organisatie en bevat geen richtlijnen voor socialemediagebruik door leden van het college en de gemeenteraad. In het algemeen gelden voor college- en raadsleden met betrekking tot het gebruik van sociale media de richtlijnen zoals vastgelegd in de voor hen geldende gedragscodes.

3.1 Gebruik

Wie werkzaam is voor de gemeente Brunssum is dat ook buiten de organisatie. Ook wanneer de medewerker zich op sociale media begeeft. Iedere uitlating op sociale media kan als gevolg daarvan in verband worden gebracht met de functie en het werk als ambtenaar bij de gemeente, en daarmee met de gemeente zelf.
Dit brengt het risico met zich mee dat door handelingen van ambtenaren op sociale media de gemeente (reputatie)schade wordt toegebracht. Dergelijke sociale media 'missers' zijn vaak het gevolg van onvoldoende besef bij de ambtenaar dat voor de buitenwereld onbedoeld de indruk kan ontstaan dat hij namens het gemeentebestuur handelt of spreekt.
Om (reputatie)schade voor de gemeente Brunssum via socialemediagedrag zoveel mogelijk te voorkomen, zijn onderstaande richtlijnen opgesteld, ter bescherming van zowel de individuele ambtenaar als de gemeente, zowel in de werksituatie als in de privé-situatie.

Zakelijk/werkplek
De gemeente Brunssum beheert een aantal socialemediakanalen, waaronder Twitter, Facebook, Instagram, WhatsApp, LinkedIn en Youtube. Het praktisch beheer van deze kanalen ligt bij het onderdeel Communicatie en Voorlichting.
Voor het gebruik van sociale media gelden de uitgangspunten die reeds in bestaand gemeentelijk beleid zijn vastgelegd. Een voorbeeld hiervan is de richtlijn "Persbeleid in Brunssum", opgenomen in het communicatiebeleidsplan "Van informeren naar communiceren" (Verseon registratiekenmerk 832001). Deze richtlijn geeft duidelijk de kaders aan voor de omgang met de media. De richtlijn bepaalt onder meer dat perscontacten een taak is die expliciet is voorbehouden aan medewerkers van het onderdeel Communicatie en Voorlichting.

De medewerker is in zijn hoedanigheid als ambtenaar niet aanwezig op sociale media

De gemeente Brunssum is aanwezig op de sociale media via de officiële kanalen. Het beheer van deze kanalen is ondergebracht bij het onderdeel Communicatie en Voorlichting. De gemeente Brunssum is op deze kanalen aanwezig als het collectief 'gemeente', en niet als individuele ambtena(a)r(en). Ook buiten deze officiële kanalen is het ambtenaren niet toegestaan zich op sociale media te manifesteren namens de gemeente Brunssum, of als ambtenaar werkzaam bij de gemeente Brunssum.
Incidenteel kunnen, op projectbasis of rondom een specifiek thema, sub-accounts worden ingericht. Ook van deze accounts is de gemeente de afzender, en geen individuele ambtenaren. Hiermee wordt voorkomen dat onze omgeving de gemeente ervaart als afzender van meervoudige, niet eenduidige, mogelijk zelfs conflicterende berichtgeving.

Berichtgeving via sociale media gebeurt alleen via de officiële accounts
Het is nadrukkelijk niet toegestaan om vanuit de eigen ambtelijke taak/functie via sociale media (daarmee ook WhatsApp) werkgerelateerde informatie te communiceren. Er is een gebrek aan controle over wie wat leest. Dit kan tot gevaarlijke situaties leiden.
Ambtenaren die vanuit hun functie oordelen dat bepaalde aan gemeente Brunssum gerelateerde informatie geschikt is om te delen via sociale media, kunnen het onderdeel Communicatie en Voorlichting van de afdeling Bestuurszaken verzoeken om deze informatie via de officiële gemeente-accounts te verspreiden, of hiervoor sub-accounts in te richten die zijn gerelateerd aan specifieke projecten of thema's.
Het staat de medewerker vrij om officiële berichten van de gemeente Brunssum te re-tweeten, te liken, of anderszins door te plaatsen of te publiceren binnen de context van de eigen sociale media.

3.2 Privé/thuis

Voor het gebruik van de sociale media in een privé-situatie geldt dat in de meeste situaties gebruikers goed aanvoelen welke gedragingen en uitlatingen acceptabel zijn. Soms, echter, kan het lastig zijn een goede afweging te maken, bijvoorbeeld:

- Iemand wil op zijn persoonlijke socialmedia-account over werkgerelateerde zaken schrijven en weet niet goed of dat mag.
- Een leidinggevende vindt dat een medewerker zich te veel profileert via sociale media en spreekt hem daarop aan.
- Een medewerker twittert uit een vertrouwelijke bijeenkomst of uit via sociale media kritiek op de eigen organisatie.

De volgende basisprincipes helpen bij het maken van de juiste afwegingen:

1. Geef, verstrek of publiceer nooit (vertrouwelijke) werkinformatie van de gemeente Brunssum (lees voor meer informatie de paragraaf "privacy").
2. Ken de huis- en gedragsregels van de gemeente Brunssum.De medewerker moet ervoor zorgen dat deze bekend is met de huis- en gedragsregels (denk aan de integriteitscode en dit protocol) van de gemeente Brunssum. Deze regels dienen als leidraad voor de omgang met collega's, klanten, ketenpartners en andere belanghebbenden. Ze zijn dan ook volledig van toepassing op activiteiten op de sociale media.
3. Blijf alert bij het mixen van privéleven en werksfeer.Online lopen werk en privé gemakkelijk in elkaar over. Een ambtenaar moet zich ervan bewust zijn dat het in het openbaar stelling nemen haaks kan staan op de belangen van de gemeente Brunssum en dat dit een conflict kan veroorzaken. Doe geen uitlatingen die de belangen, het imago en de geloofwaardigheid van de gemeente kunnen aantasten, of die afbreuk doen aan het eigen functioneren als ambtenaar. Een van de grondregels bij het voorkomen van een ongewenste vermenging van privé-uitlatingen en de belangen van werk en werkgever is deze: hoe dichter het onderwerp waarover de medewerker zich uitlaat bij zijn/haar eigen functie ligt, des te meer de medewerker moet opletten met uitlatingen.
4. De medewerker dient rekening te houden met het feit dat hij/zij zich begeeft in een sociale omgeving.De medewerker moet bedachtzaam zijn dat hij/zij de leidinggevende, de collega's en de klanten deelgenoot maakt van het vertoonde gedrag in een sociale ruimte (online dan wel offline). Goede manieren zijn belangrijk. Zorg dat acties en gedrag overeenkomen met normen die gelden voor de ambtenaar, en bij een professionele, dienstverlenende organisatie als de gemeente Brunssum. De medewerker dient er rekening mee te houden dat online berichten een permanent en openbaar karakter hebben. Men weet niet wie er meeleest.
5. Voorkom verwarring, gebruik een disclaimer. Heeft u een eigen twitter-account, Facebook-pagina, blog of website, voorkom dan dat de indruk voor de buitenwacht ontstaat dat het een communicatiekanaal van de gemeente Brunssum betreft. Waar geventileerde meningen en opvattingen via deze privé-media het werk van de gemeente raken, moet duidelijk zijn dat de inhoud van het betreffende kanaal persoonlijke opvattingen en meningen zijn. Dat kan in de vorm van een disclaimer.
6. De medewerker is altijd ambassadeur van de gemeente Brunssum. Ambtenaren zijn de ambassadeurs van de gemeente Brunssum, óók op sociale media. Het staat de medewerker vrij om officiële berichtgeving van de gemeente Brunssum te liken of om deze berichten op de eigen

persoonlijke pagina's te delen. Als de medewerker twijfelt over een toelichtende tekst, deel het bericht zonder eigen commentaar toe te voegen.
7. Vermijd (impulsieve) reacties. Als de medewerker berichten van de gemeente Brunssum doorplaatst of deelt, hou er rekening mee dat dit reacties kan uitlokken. Indien de medewerker negatieve berichten signaleert, stuur deze dan naar de eigen leidinggevende en/of de socialmediaredacteur. Vermijd een eigen (impulsieve) reactie teneinde escalatie van de discussie te voorkomen.
8. In geval van twijfel: vraag! Alles wat een ambtenaar plaatst en publiceert, is uiteindelijk de eigen verantwoordelijkheid. Bij twijfel: plaats geen bericht of vraag advies bij de eigen leidinggevende of door een medewerker van het onderdeel Communicatie en Voorlichting.

4. Beveiliging

1. Ten behoeve van de bestrijding van virussen e.d. wordt alle ontvangen externe e-mail automatisch gescand op virussen en op zogenaamde "spam" (ongewenste e-mail). De verzender ontvangt tevens een bericht dat zijn e-mail een virus bevat. Ongewenste e-mail wordt via een filter tegengehouden en eventueel niet meer doorgezonden naar de geadresseerde. Dit om overbelasting van het e-mailsysteem te voorkomen.
2. Gebruik overal een veilig wachtwoord dat niet makkelijk te raden is en bij voorkeur bestaat uit een combinatie van letters, cijfers, leestekens en minimaal 8 tekens lang is. Plak geen post-its met wachtwoorden op of bij de eigen werkplek. Doe ook geen aanwijzingen in de tas van de laptop. Als de medewerker deze tas mee naar buiten neemt en hij in (tijdelijk) bezit van een ander komt kan deze toegang krijgen tot het gemeentelijke netwerk.
3. Alertheid en het herkennen van een verdachte (phishing) e-mail en vervolgens snel en adequaat handelen door medewerkers is van cruciaal belang om calamiteiten te voorkomen. "Phishing" is een vorm van internetfraude waarbij men valse e-mails ontvangt die de ontvanger van de e-mail naar een nagebootste website proberen te lokken. Het is vaak moeilijk een phishing e-mail te onderscheiden van een echte e-mail. Toch zijn er wel kenmerken waaraan een phishing e-mail is te herkennen. Controleer het e-mailadres van de afzender, controleer aanhef, taalgebruik en/of spelling en spot urgentie. Open deze e-mails niet, klik niet op een verdachte link of bijlage en geef nooit zomaar persoonlijke gegevens. Waarschuw per direct support telefonisch of per e-mail. Laat support de verdachte e-mail verwijderen. Neem bij twijfel altijd contact op met support, meld uw incident/vraag/opmerking en laat het registreren.
4. Van de medewerker wordt geacht dat het computerscherm gelockt wordt als deze de werkplek verlaat. Het locken van het scherm kan via het gelijktijdig indrukken van de toetsen [Win] + [L]. (De [Win]-toets is de toets met het Windows-logo tussen de Ctrl- en Alt-toets.)
5. Sluit een usb-stick of andere gegevensdragers met onbekende herkomst niet aan op de computer. Deze moeten altijd aan support afgegeven worden. Support controleert ze en stelt de informatie beschikbaar. Indien de gegevensdrager privacygevoelige informatie bevat moet de medewerker dit aan support of DIV melden. Er zijn in de organisatie een aantal medewerkers die bevoegd zijn om deze gevoelige informatie te openen en te beoordelen.
6. Wanneer de medewerker niet via een vaste interne werkplek werkt, moet deze gebruik maken van een beveiligde verbinding, dus niet van een openbaar (wifi-)netwerk.
7. Geef iemand niet zomaar toegang tot een zakelijk wifi-netwerk. Voor bezoekers van de gemeente Brunssum kan de medewerker een gastenpas aanmaken om de gasten toegang te verlenen aan ons beveiligde wifi-netwerk (zie "Handleiding gastenpas aanmaken (Govroam)").
8. Indien ondanks alle beveiligingsmaatregelen er toch schadelijke zaken binnendringen op de werkplek-computer en/of op het interne netwerk dient hiervan onverwijld een leidinggevende van de afdeling Informatiemanagement in kennis gesteld te worden. Preventief kunnen bepaalde sites/nieuwsgroepen van het internet worden afgesloten of bepaalde vormen van internetgebruik worden voorkomen door de gemeente. Dit gebeurt op basis van "content filtering".

5. Privacy

Per 25 mei 2018 wordt de AVG gehandhaafd. De AVG zorgt onder meer voor: versterking en uitbreiding van privacyrechten, meer verantwoordelijkheden voor organisaties; dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.
Dit komt neer op meer zorgvuldigheid, het treffen van technische en organisatorische maatregelen en meer rechten. Dit alles staat in dienst van informationele privacy: de bescherming van persoonsgegevens, m.n. het recht om niet meer informatie over zichzelf te verstrekken en aan niet meer personen dan strikt noodzakelijk is, en het recht om te weten welke persoonlijke informatie er in omloop is, hoe die verzameld is en wat ermee gedaan wordt. De gemeente speelt hier een belangrijke rol in.

Alle maatregelen in het kader van de bescherming van gegevens hebben natuurlijk weinig zin als ze niet in een veilige omgeving verwerkt worden. De AVG stelt daarom niet alleen eisen aan de data zelf, maar juist ook aan de veiligheid van de verwerkingsverantwoordelijke, in dit geval, de ambtenaren. Vier specifieke maatregelen uit de AVG zijn versleuteling (beveiliging), garantie (het systeem moet betrouwbaar zijn), herstel (de problemen die zich voordoen moeten zo snel mogelijk worden opgelost) en procedure (het testen en evalueren van de veiligheid).
In deze paragraaf wordt er eerst ingegaan op de privacy van de medewerker zelf bij onrechtmatig gebruik van de gemeentelijke voorzieningen, daarna wordt het omgaan met privacygevoelige informatie besproken. Op de website van gemeente Brunssum kan de privacyverklaring worden ingezien: Home / Bestuur en Organisatie / Over deze website / Privacyverklaring.

5.1 Eigen privacy

1. De gemeente zal geen persoonsgegevens over e-mail en internetgebruik, zoals tijdsbesteding, data, afzenders, inhoud, bezochte sites, e.d. actief monitoren en vastleggen. Dit laat onverlet dat controles op incidentele basis kunnen plaatsvinden vanwege meer zwaarwichtige redenen, zoals bij verdenking van o.a. financiële schendingen, misbruik positie en belangenverstrengeling, lekken en misbruik van informatie, misbruik bevoegdheden, misbruik geweldsbevoegdheid, ongewenste omgangsvormen, misbruik bedrijfsmiddelen en overschrijding interne regels en strafbare misdragingen buiten werktijd. Opdrachten voor dergelijke controles vinden altijd plaats in opdracht van de gemeentesecretaris in overleg met het afdelingshoofd Informatiemanagement. Bij constatering van misbruik wordt steeds achteraf melding gemaakt bij de ondernemingsraad. De secretaris of directeur voert samen met de aangewezen functionaris en eventueel diens leidinggevende met de betrokken medewerker een gesprek om aan te geven dat er een vermoeden van een misstand over hem gemeld is en dat dit aanleiding is of kan zijn tot een onderzoek. De mogelijke verdere consequenties staan beschreven in “Procedure voor het verrichten van een onderzoek bij een vermoeden van misstand” (Verseon bijlage van het BBV 375319 met registratiekenmerk 375448).
2. Een aantal medewerkers van de afdeling Informatiemanagement hebben uit hoofde van hun functie meer rechten op het interne netwerk dan overige medewerkers. Ze hebben vanuit de aard van hun functie dan ook een geheimhoudingsplicht. Zij zijn niet bevoegd tot het ongevraagd meekijken bij het internetgebruik van andere medewerkers. Alleen de gemeentesecretaris is in overleg met het afdelingshoofd Informatiemanagement bevoegd de medewerkers van Informatiemanagement bijzondere opdrachten te verstrekken om bepaalde zaken op het netwerk bij verdenking van onrechtmatig gebruik nader te controleren of daarover informatie te verschaffen.
3. Bij onvoorziene, langdurige afwezigheid kan de werkgever (leidinggevende, directe (ex-)collega’s of een benoemd intern vertrouwenspersoon) de persoonlijke e-mailbox van de betreffende werknemer inzien. Het belang en de urgentie voor de werkgever is hoog om toegang te krijgen tot lopende zaken. Hij moet een gerechtvaardigd belang hebben bij controle van de werknemer. Dat belang moet de controle en de wijze waarop die plaatsvindt rechtvaardigen in verhouding tot de inbreuk die op de privacy van de werknemer wordt gemaakt. Concreet: de wijze van controle moet in verhouding staan tot het doel (eis van proportionaliteit) en het doel mag niet bereikbaar zijn op een wijze die minder inbreuk maakt op de privacy (eis van subsidiariteit). Bij een verzoek om toegang te verlenen tot de persoonlijke e-mailbox van een medewerker, wordt dit eerst voorgelegd voor advies en besluitvorming aan het team bestaande uit de functionaris informatiebeveiliging, de functionaris gegevensbescherming, het afdelingshoofd van Informatiemanagement en een interne vertrouwenspersoon. Dit team zorgt gezamenlijk voor een aantoonbaar advies en besluit. Daarna bewerkstelligt de afdeling Informatiemanagement pas de verdere technische realisatie.
4. Als sprake is van een situatie zoals beschreven in lid 3, mag de werkgever de zakelijke e-mails uit de persoonlijke e-mailbox lezen. De medewerker kan zelf onderscheid maken tussen de zakelijke e-mails en de privé-e-mails. De medewerker kan dit doen door de privé-e-mail in een aparte map te bewaren (bijvoorbeeld met de titel ‘Persoonlijk’). Of door bij privé-e-mails ‘persoonlijk’ in de titel van het bericht te zetten. Blijkt uit de titel van het bericht dat de e-mail persoonlijk is? Dan mag de werkgever dat bericht niet lezen. Is er geen scheiding gemaakt tussen zakelijke en privé-e-mail? Dan moet de werkgever er rekening mee houden dat werknemers privéberichten ontvangen en versturen. Bij het lezen van de e-mail van de betreffende medewerker moet de werkgever de privéberichten zo veel mogelijk ontzien.

5.2 Omgaan met privacygevoelige informatie

1. Ga zorgvuldig om met 'gegevensdragers' zoals usb-sticks, losse harde schijven, dvd's, maar ook smartphones en tablets; berg ze goed op en raak ze niet kwijt. Beveilig deze gegevensdragers zo veel mogelijk met een wachtwoord (een beveiligde usb-stick voor het uitwisselen van vertrouwelijke gegevens is bij support te verkrijgen).

2. Verwijder alle bestanden met persoonsgegevens van lokale apparatuur en externe apparaten na afloop van een project.
3. E-mail en sociale media zijn niet 100% veilig voor het uitwisselen van informatie. Om alsnog privacygevoelige informatie te delen, kan de medewerker gebruikmaken van de ingebouwde plug-in in Outlook. Op dit moment is dat voor onze organisatie Cryptshare. In de handleiding voor het gebruik van Cryptshare is een beslisboom opgenomen die de medewerker kan raadplegen om te beslissen wanneer iets versleuteld verstuurd dient te worden (zie "Handleiding Cryptshare gemeente Brunssum").
4. Let op als e-mails verstuurd worden: zijn de juiste personen geadresseerd? Is het wenselijk dat ze elkaars e-mailadressen zien? Zo nee, adresseer ze via BCC (Blind Copy).
5. Plaats geen persoonsgegevens of vertrouwelijke gemeentelijke data in een cloud-oplossing, zoals WeTransfer, Dropbox, enzovoorts.
6. Bij gemeente Brunssum is er een "clean desk"-beleid. Het is te alle tijden niet toegestaan vertrouwelijke informatie op het bureau van de medewerker te laten liggen.
7. Deponeer papier met vertrouwelijk informatie in de aluminium papiercontainers. De containers staan in de pantry op de etages 3 tot en met 7, bij college B&W, bestuurssecretariaat, burgerzaken locatie Lindeplein, Boschstraat (1 container) en in het oude gemeentehuis (1 container). Deze aluminium containers vormen een gesloten papiercircuit voor het gecertificeerd laten afvoeren en vernietigen van papieren documenten. Kopieën of printafdrukken van originele documenten deponeert de medewerker in deze container. Originele documenten worden nooit weggegooid. Deze worden door het cluster DIV van de afdeling Informatiemanagement behandeld.
8. Privacygevoelige documenten dienen alleen op een beveiligde printer te worden geprint. De meeste medewerkers van de Gemeente Brunssum maken gebruik van de follow-me en de beveiligde printeromgeving. Dit heeft als voordeel dat printopdrachten pas geprint worden als de medewerker bij de printer staat en zich aanmeldt als de eigenaar van het document. Zo kunnen de vertrouwelijke documenten van de medewerker niet in verkeerde handen komen. Kies "PR_Brunssum op hln…" als standaard printer. Als de standaard printer om welke reden dan ook is gewijzigd, kies dan heel bewust opnieuw voor deze beveiligde printer "PR_Brunssum op hln…". Als de medewerker alsnog iets via een niet beveiligde printer afdrukt, dan dient de medewerker meteen actie te ondernemen en ervoor te zorgen dat de afdrukken opgehaald worden. Daarnaast neemt de medewerker contact op met de functionaris gegevensbescherming of de functionaris informatiebeveiliging om samen te beoordelen of er sprake is van een datalek.
9. Bij onverhoopt verlies van potentieel privacygevoelige data (zowel analoog als digitaal), dan is dit een datalek en moet dit zo snel mogelijk worden gemeld. Het incident wordt eerst door de functionaris gegevensbescherming en/of de functionaris informatiebeveiliging beoordeeld. Als het inderdaad gaat om een datalek, wordt dit binnen 72 uur na ontdekking door de functionaris gegevensbescherming gemeld bij de AP (Autoriteit Persoonsgegevens). We spreken van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Denk daarbij aan uitgelekte computerbestanden, een e-mail verzonden naar verkeerde adressen, een gestolen laptop of een verloren usb-stick. Ook een gestolen geprinte personenlijst kan een datalek zijn. Een datalek moet worden gemeld als het leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Persoonsgegevens zijn alle gegevens over een natuurlijk persoon. Dus niet alleen naam, adres, telefoonnummer, maar ook BSN, geslacht, seksuele geaardheid, godsdienst, politieke overtuiging, foto, gezondheidsgegevens, enzovoort. Een datalek kan grote gevolgen hebben. Voor de persoon of personen in kwestie is het bijzonder vervelend dat zijn gegevens in verkeerde handen vallen, het is een schending van zijn privacy. Van de informatie kan ook misbruik worden gemaakt, denk aan identiteitsdiefstal. Ook kan er sprake zijn van reputatieschade van gemeente Brunssum. Tot slot kan een datalek leiden tot enorme boetes.

Verwijzingen

Deze regeling is gebaseerd op en verwijst naar de volgende documenten:

- AVG-wetgeving, verdere informatie is te vinden op https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/algemene-informatie-avg
- "Beveiligd printen en kopiëren" te vinden op Intranet
- "E-mailgedragslijn voor overheden: 'altijd antwoord, tijdig antwoord'" te vinden op https://www.overheid.nl/contact/e-mailgedragslijn-voor-overheden
- "Gecertificeerd afvoeren en vernietigen van papieren documenten", te vinden op Intranet
- "Gemeentelijke gedragscode gebruik E-mail en Internet" (2008) te vinden bij RAP
- "Handleiding Cryptshare gemeente Brunssum" te vinden op Intranet
- "Handleiding gastenpas aanmaken (Govroam)" te vinden op Intranet
- "Handboek heldere teksten schrijven" (2018) te vinden op Intranet

- “Inzage door werkgever in persoonlijke mailbox werknemer” (2017)
- “Nota integriteitbeleid” (2012) te vinden in RAP
- “[Outlook 2016] Handleiding machtigingen instellen” te vinden op Intranet
- “[Outlook 2016] Instructie automatisch antwoorden bij afwezigheid/vakantieregel instellen” te vinden op Intranet
- “Persbeleid in Brunssum”, opgenomen in het communicatiebeleidsplan “Van informeren naar communiceren” te vinden in Verseon onder kenmerk 832001
- “Phishing Security Test” te vinden op Intranet
- “Privacybeleid 2018-2021” (2018), concept versie
- “Procedure tot het verrichten van een onderzoek bij een vermoeden van misstand” te vinden in Verseon, bijlage 375448 bij het BBV 375319 (B&W 27-11-2012)
- “Richtlijnen voor het gebruik van social media gemeente Brunssum” (2012) te vinden in RAP
- “Selectie verkeerde printer wordt potentieel Datalek” te vinden op Intranet
- Vervangingsbesluit, te vinden in Verseon onder kenmerk 561857