# HUISREGELS GEMEENTE BOEKEL

Hieronder staan diverse afspraken die we binnen onze organisatie hebben afgesproken. Het zijn regels over hoe je omgaat met bedrijfsmiddelen, hoe je privéapparatuur mag gebruiken voor zakelijk gebruik, het verstrekken van gegevens via de telefoon, alcohol en drugsgebruik, kledingvoorschriften, het maken van opnames, het melden van beveiligingsincidenten en datalekken en het opslaan van vertrouwelijke informatie op verwijderbare media zoals een USB-stick.


***Deze afspraken zijn van toepassing op alle medewerkers en bestuurders van de gemeente Boekel.***

## 1. Aanvaardbaar gebruik bedrijfsmiddelen

- Medewerkers gaan met de aan hen ter beschikking gestelde bedrijfsmiddelen zorgvuldig, met respect en integer om. Bij het gebruik van bedrijfsmiddelen brengen medewerkers de goede naam en de reputatie van de gemeente Boekel of de medewerkers van de gemeente niet in gevaar.
- Toegang tot de mobile devices dient beveiligd te worden met pincode en/of wachtwoord conform het wachtwoordbeleid.
- Mobile devices worden door I&A voorzien van voorzieningen om het device bij verlies en/of diefstal te kunnen opsporen en op afstand de gemeentelijke informatie te verwijderen.
- Op mobile devices waarop ook gemeentelijke informatie wordt opgeslagen en/of benaderd, dient antivirus software geïnstalleerd te worden door de gebruiker van het device, indien deze niet centraal beheerd worden door I&A. Tevens worden deze devices onmiddellijk na het vrijgeven voorzien van updates.
- Medewerkers gebruiken bedrijfsmiddelen op een efficiënte manier en nemen redelijke en gepaste maatregelen om kosten of schade voor de gemeente Boekel te beperken / te voorkomen. Medewerkers voorkomen ongeoorloofd gebruik van bedrijfsmiddelen.
- Verwijderbare media (cd's, USB-sticks, schijven, etc.) en informatiedragers zoals laptops, smartphones, tablets e.d. met vertrouwelijke en/of privacygevoelige informatie mogen niet onbeheerd worden achtergelaten op plaatsen die toegankelijk zijn zonder toegangscontrole. Verlies en zoek raken van bedrijfsmiddelen / gegevensdragers dient gemeld te worden als incident aan zowel de leidinggevende als de coördinator I&A (Caroline Kat) en de medewerker informatiebeveiliging & privacy (Frank Schaap). Verlies van deze media en informatiedragers kan een datalek zijn dat z.s.m. moet worden doorgegeven aan deze medewerkers.
- Defecte informatiedragers (usb-sticks, cd/dvd, mobile devices, tablets e.d.) worden ingeleverd bij I&A.
- Het meenemen van vertrouwelijke of vergelijkbaar geclassificeerde informatie buiten het gemeentehuis vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is. Indien informatiedragers (laptop, tablet, telefoon, papieren dossiers etc.) extern worden meegenomen, moeten ze dusdanig worden gebruikt, beheerd en opgeslagen dat vertrouwelijke informatie niet beschikbaar kan komen voor onbevoegde personen.

Onder ongeoorloofd gebruik van bedrijfsmiddelen wordt verstaan:

- Het bezoeken, downloaden, verspreiden van internetfaciliteiten met een pornografische en discriminerende inhoud.

- Het versturen van berichten aan een groot aantal ontvangers, kettingbrieven en kwaadaardige virussen, spyware en Trojaanse paarden.
- Het downloaden en/of verzenden van illegale software.
- Online gokken.
- Online spelen van spellen.
- Het zonder toestemming van I&A installeren of pogen daartoe van software in de netwerkomgeving.

## 2. Bring your own device (BYOD)

De gemeente Boekel staat de volgende privéapparatuur toe voor zakelijk gebruik:

- Mobiele telefoons
- Smartphones
- Laptops
- Tablets

Het aansluiten van bovengenoemde apparatuur is slechts toegestaan op de daarvoor beschikbaar gestelde (draadloze) netwerkaansluitingen.

Zakelijk gebruik van bovengenoemde apparatuur is slechts toegestaan indien deze zijn voorzien van:

- Wachtwoordauthenticatie.
- Een actuele virusscanner en firewall.
- Automatische schermbeveiliging/blokkering van het scherm na 10 minuten inactiviteit.

Eindgebruiker is hiervoor zelf verantwoordelijk, evenals voor het updaten, inrichten en oplossen van problemen met het apparaat en software.

Indien op de privéapparatuur ook zakelijke gegevens staan opgeslagen, mag deze apparatuur niet ongeoorloofd gebruikt worden als bedoeld onder de kop ‘aanvaardbaar gebruik bedrijfsmiddelen’.

## 3. Gegevens verstrekken via de telefoon

Het uitgangspunt is dat niet aan verzoeken wordt tegemoet gekomen om telefonische informatie over betrokkenen te communiceren. Er kan informatie verstrekt worden aan derden via de telefoon, mits de identiteit van deze derde voldoende is vastgesteld (bijv. door middel van zelf terug te bellen via een centraal telefoonnummer) en een schriftelijk verzoek tot informatie niet mogelijk is. Informatie waarvan de gemeente geen bronhouder is (bijvoorbeeld kadaster en handelsregister) mag nooit aan derden worden verstrekt. Ook persoonlijke gegevens van collega’s (vakanties, ziekte, adres, privé telefoonnummers, etc.) mogen niet verstrekt worden aan derden.

## 4. Alcohol, medicijnen en drugs

Het nuttigen van alcohol (behoudens door de gemeente georganiseerde borrels) en drugs, evenals het onder invloed zijn van alcohol en drugs tijdens het uitvoeren van werkzaamheden wordt binnen de Gemeente Boekel niet getolereerd. Voor verdere informatie zie het protocol alcohol, medicijnen en drugs.

*Gebruik medicijnen*

Medewerkers die op doktersvoorschrift geneesmiddelen gebruiken die de rijvaardigheid of het functioneren beïnvloeden, dienen de direct leidinggevende hiervan in kennis te stellen.

## 5. Kledingvoorschriften

Binnen de Gemeente Boekel gelden in principe geen kledingvoorschriften. Er wordt verwacht dat iedere medewerker zich representatief kleedt en voor een verzorgd uiterlijk zorg draagt. De Gemeente Boekel behoudt zich het recht voor om de medewerker aan te spreken op diens manier van kleden en/of persoonlijke hygiëne.

## 6. Maken van opnames

Zonder expliciete toestemming van een leidinggevende mogen binnen het gemeentehuis geen opnames (foto, video of geluid) worden gemaakt.

## 7. Melden van beveiligingsincidenten en datalekken

Elke medewerker van de gemeente Boekel (zowel tijdelijk, vast als extern) is verplicht een vermoedelijk beveiligingsincident of datalek direct mondeling of schriftelijk te melden aan zijn direct leidinggevende (of contactpersoon bij de gemeente) en de medewerker informatiebeveiliging & privacy. Een dergelijke verplichting is gericht op tekortkomingen in de beveiliging zo snel mogelijk te ontdekken en te kunnen oplossen. Tevens zijn medewerkers verplicht onvolkomenheden in de programmatuur (of vermoeden daarvan) op het terrein van beveiliging te melden.

<u>Wat wordt verstaan onder een datalek?</u>
Gedacht kan worden aan de volgende voorbeelden:

- Een aanval op het netwerk;
- Diefstal of verlies van een laptop, USB-stick of telefoon;
- Gestolen papieren (patiënten)dossier(s);
- Onjuiste adressering van e-mail of fysieke post met persoonsgegevens;
- Tekortschietende beveiliging van bestanden of gegevens;
- Slordig omgaan met het beheer van wachtwoorden;
- Het openbaar publiceren van privacygevoelige informatie.

## 8. Opslag van vertrouwelijke informatie op verwijderbare media

De gemeente biedt usb-sticks aan. Deze sticks zijn echter niet beveiligd. Daarom mag hier geen vertrouwelijke informatie op worden opgeslagen. Daarnaast worden er aan bepaalde personen vanwege de functie tablets en telefoons verstrekt. Deze apparaten dienen beveiligd te worden met een sterk wachtwoord en schermblokkering na 10 minuten inactiviteit. Verder dient het apparaat voorzien te zijn van een actuele virusscanner, firewall en voorziening om het apparaat na diefstal en/of zoek raken te kunnen lokaliseren en te wissen. Omdat de interne bestanden op het interne netwerk verder niet beveiligd zijn, moeten de vertrouwelijke bestanden die op een usb-stick en/of apparaat worden geplaatst van een wachtwoord worden voorzien, bijvoorbeeld met een zip-programma.

Alle devices dienen voorzien te zijn van een sterk wachtwoord en/of pincode van minimaal 4 verschillende, niet opeenvolgende cijfers / letters. Zoekgeraakte en/of gestolen apparaten dienen onmiddellijk te worden gemeld bij de leidinggevende en de medewerker informatiebeveiliging & privacy. Defecte devices en opslagmedia dienen bij de coördinator I&A te worden ingeleverd, zodat voor een veilige vernietiging kan worden gezorgd.