ICT gedragscode

DOEL: **het stellen van regels over het verantwoord gebruik van internet en e-mail, zodat ICT veilig, snel, flexibel en betrouwbaar wordt gehouden.**

REIKWIJDTE: **alle medewerkers, die ICT middelen ter beschikking krijgen gesteld van Koninklijke Oosterhof Holman (KOH).**

AANSPREEKBAARHEID: **elke medewerker wordt geacht de inhoud van de ICT gedragscode te kennen en zich hier aan te houden, waarop het Sanctiebeleid KOH van toepassing is.**

Inleiding

Elke organisatie heeft tegenwoordig informatie- en communicatietechnologie (ICT) nodig om het werk uit te oefenen. Hiervoor worden allerlei ICT middelen ter beschikking gesteld. Aan het gebruik van ICT zijn risico's verbonden, die het stellen van gedragsregels noodzakelijk maken. Onder 'ICT-middelen' wordt verstaan: alle middelen die een rol vervullen in informatie- en communicatieprocessen. Het gaat hierbij onder meer om PC's/laptops, (mobiele) telefoons, printers, informatiedragers, kopieerapparatuur, scanners, modems, internettoegang, e-mail en programma's/computersoftware. Onder 'gegevens' wordt verstaan: alle informatie die zich al dan niet tijdelijk bevindt op ICT-middelen van KOH. Dit is alle informatie die gemaakt, ontvangen, vermenigvuldigt, gewijzigd en/of verstuurd wordt door gebruik te maken van ICT-middelen.

1. Internet en email

1.1 Aan de medewerker wordt het gebruik van internet, intranet en e-mail toegestaan, zodat de medewerker alle informatie kan verzamelen, die hij nodig heeft om zijn werkzaamheden goed te kunnen uitvoeren.

1.2 De medewerker bekijkt, vertoont, download en/of verspreidt geen bestanden en/of beelden, die ten nadele zijn van de organisatie, dan wel de grenzen van betamelijkheid en fatsoen overschrijden.

1.3 De medewerker bezoekt geen onoorbare sites, waaronder in ieder geval begrepen sites, die pornografisch en/of racistisch materiaal bevatten.

1.4 Het is de medewerker niet toegestaan om e-mails te verzenden met een pornografische, racistische, discriminerende, beledigende, aanstootgevende en/of (seksueel) intimiderende inhoud en die (kunnen) aanzetten tot haat en/of geweld.

1.5 De medewerker gebruikt e-mail volgens de regels overeenkomstige stoffelijke correspondentie, het grondwettelijk briefgeheim daarbij inbegrepen.

1.6 Indien een e-mail naar een groep wordt verstuurd, dient de medewerker deze mailadressen toe te voegen in de BCC om onnodig ongewenste (privé) e-mailadressen uit te wisselen.

1.7 Alle e-mail bevat automatisch een disclaimer van KOH en is voorzien van e-mail handtekening van de afzender.

1.8 Voor het gebruik van social media wordt verwezen naar het KOH Social media en persbeleid.

2. Beveiliging en gebruik

2.1 De beschikbaar gestelde ICT-middelen en gegevens zijn primair bedoeld voor zakelijk gebruik en blijven te allen tijde eigendom van KOH.

2.2 Toegang tot het KOH-netwerk is alleen toegestaan met ICT middelen, die zijn ingericht volgens KOH-standaarden en -eisen.

2.3 De door KOH verstrekte gebruikersnaam en wachtwoord zijn persoonsgebonden en mogen niet aan anderen ter beschikking worden gesteld.

2.4 Het KOH-gebruikerswachtwoord moet voldoen aan de volgende voorwaarden:
- Minimaal 12 tekens
- Minimaal 1 hoofdletter
- Minimaal 1 cijfer
- Minimaal 1 speciaal teken
- Geen voor- en achternaam
- Geen eerder gebruikt wachtwoord

2.5 Voor zakelijke (web)applicaties welke niet aan het KOH-account gekoppeld zijn, is het advies een wachtwoordmanager te gebruiken. Vraag bij de ICT naar de mogelijkheden.

2.6 Een systeem, waarop de medewerker heeft ingelogd, moet worden afgesloten bij het einde van het gebruik en mag door de medewerker nimmer onbeheerd worden achtergelaten.

2.7 Beveiligings- en gebruiksaanwijzingen van de Afdeling ICT dient de medewerker altijd op te volgen.

2.8 In geval medewerker eigen hardware, software, mobiele telefonie en/of smartphone en /of andere middelen wenst te gebruiken ten behoeve van zijn werkzaamheden voor KOH, zal medewerker daar toestemming voor vragen aan KOH. Alle relevante bepalingen uit onderhavig reglement zijn daarop van toepassing.

2.9 Aanvragen voor nieuwe hard- en/of software dient de medewerker in te dienen via: https://servicedesk.oosterhofholman.nl

2.10 Medewerker zal zonder toestemming van KOH geen vertrouwelijke informatie of informatie, waar intellectuele eigendomsrechten op rusten, op eigen initiatief buiten het bedrijfsnetwerk van KOH brengen.

2.11 De volgende handelingen betreffende het computer- en netwerkgebruik zijn voor de medewerker alleen toegestaan in overleg met Afdeling ICT:

- wijzigen van de computerconfiguratie;
- verplaatsen van de hardware;
- installeren of downloaden van software;
- aansluiten van externe apparatuur;
- zelf verhelpen van storingen, onregelmatigheden, e.d.

2.12 Het is de medewerker niet toegestaan handelingen te verrichten, die gericht zijn op het aanmaken, binnenhalen, en/of verspreiden van virussen in welke vorm dan ook, almede handelingen te verrichten die gericht zijn op het ongewenst benaderen en/of binnendringen van computers en computersystemen (hacken);

2.13 De medewerker is verantwoordelijk voor het afdrukken van gegevens op printers en zal de vertrouwelijkheid van afgedrukt materiaal waarborgen.

2.14 Het is niet toegestaan om vertrouwelijke of privacygevoelige informatie buiten het KOH netwerk te verzenden of op te slaan. Dit geldt voor e-mail (Hotmail, Gmail, Outlook.com etc.), het gebruik van diensten voor het verzenden van grote bestanden (WeTransfer, etc.) en andere diensten waarbij informatie buiten het KOH netwerk wordt opgeslagen (Prezi, Google drive, Dropbox, Onedrive, iCloud etc.). Toegestaan zijn opslag in beheer van KOH, zoals Onedrive for Business, Sharepoint en lokale Fileserver.

2.15 Ter beschikking gestelde ICT-middelen mogen zonder voorafgaande en schriftelijke toestemming van KOH niet aan derden in gebruik worden gegeven. Evenmin mogen een of meer kopieën van programmatuur aan derden worden verstrekt.

2.16 Bij geconstateerde (beveiligings)incidenten heeft de afdeling ICT het recht om apparatuur en/of medewerkers de toegang tot computers en/of netwerken (tijdelijk) te ontzeggen.

3. Externe toegang

3.1 De medewerker zal bij de uitoefening van zijn werkzaamheden, waarbij externe toegang tot informatiesystemen gebruikt wordt, de grootst mogelijke zorgvuldigheid in acht nemen.

3.2 Het gebruik van openbare wifi netwerken dient vermeden te worden.

3.3 De medewerker neemt maatregelen om te voorkomen dat derden informatie te zien krijgen, die niet voor hen bestemd is.

3.4 De Afdeling ICT verstrekt informatie over de wijze waarop externe toegang verkregen kan worden.

4. Controle

4.1 KOH is, met inachtneming van de wettelijke voorschriften ten aanzien van bescherming van de persoonlijke levenssfeer, in het bijzonder de privacywetgeving Algemene verordening gegevensbescherming (AVG), bevoegd controles uit te oefenen op het gebruik van internet en e-mail. Het doel van deze controles is de naleving van dit reglement vast te stellen.

4.2 De controle op persoonsgegevens over e-mail en internetgebruik vindt plaats met als doel

a) Voorkomen van negatieve publiciteit
b) Tegengaan van seksuele intimidatie
c) Controle op bedrijfsgeheimen
d) Systeem en netwerkbeveiliging
e) Kosten en capaciteitsbeheersing
f) Tegengaan van discriminatie

4.3 Bij constatering van verboden gebruik wordt dit onmiddellijk met de betrokken medewerker besproken door de direct leidinggevende, waarbij het KOH Sanctiebeleid van toepassing is.

5. Melden van storingen, incidenten

5.1 De medewerker dient storingen, onregelmatigheden, inbreuken op de beveiliging, ongeautoriseerd gebruik, etc. direct te melden aan de Afdeling ICT via 5.1, 2, i@oosterhofholman.nl of 5.1, 2, e

5.2 Meldingen worden geregistreerd in een geautomatiseerd administratie-/bewakingssysteem en zo mogelijk direct telefonisch verholpen. Hiervoor beschikt de IT-medewerker over een programma, waarmee het mogelijk is om de ICT-middelen over te nemen vanaf zijn eigen werkplek.

5.3 Bij constatering van misbruik en/of het gebruik van ICT-middelen, wat in strijd is met de ICT gedragscode, moet daarvan melding worden gemaakt bij de Afdeling ICT via het Schendingsformulier. Er kan een sanctie worden opgelegd, conform het KOH Sanctiebeleid.

5.4 In geval van schade, vermissing of diefstal van ICT-middelen dient de Afdeling ICT onverwijld op de hoogte worden gesteld. Indien er sprake is van inbraak en/of diefstal, dient bij de politie aangifte te worden gedaan en van het betreffende proces-verbaal een afschrift aan de Afdeling ICT te worden overgelegd.

5.5 Meldplicht Datalekken: er is sprake van een datalek wanneer een onbevoegde inzage heeft gehad via ICT-middelen in persoonsgegevens of als persoonsgegevens per ongeluk zijn vernietigd of gewijzigd. Voorbeelden van mogelijke datalekken: een verloren USB-stick met persoonsgegevens, een gestolen laptop, tablet of telefoon, een

inbraak in een databestand. Meld een (mogelijk) datalek direct bij de afdeling ICT [redacted]@oosterhofholman.nl). Zie ook KOH Privacyreglement.