# ICT gedragscode Van de Velde NV

| | | |
|---|---|---|
| Last saved on:<br>17/05/2022 | Document owner:<br>People & Organisation | Document name:<br>ICT gedragscode Van de Velde NV<br>Versie mei 2022 |

# INHOUDSTAFEL

# 1. ALGEMEEN

## DOELSTELLING EN ALGEMEEN KADER

Van de Velde draagt integriteit hoog in het vaandel. Hiertoe is de algemene gedragscode (Code of Conduct) opgesteld waarin belangrijke elementen van gewenst gedrag zijn opgenomen. Deze algemene gedragscode kan men steeds raadplegen via de Conversation Room (Files - Van de Velde NV - Guidelines/Policies). In een veranderende digitale wereld waarin het gebruik en het belang van data en ICT toenemen, zijn bijkomende richtlijnen tav data en ICT-middelen een noodzaak.

Voor de uitvoering van hun taken, stelt Van de Velde haar medewerkers data en ICT-middelen ter beschikking zoals informatie, apparatuur, internet, intranet, e-mail. Indien dergelijke middelen niet correct gebruikt worden, kan dit ongewenste effecten hebben op zowel de medewerker als de organisatie.

Onderhavige ICT-gedragscode is een gedetailleerde uitwerking specifiek voor het gebruik van deze middelen en een aanvulling op de algemene gedragscode. De ICT-gedragscode brengt het minimaal gewenste gedrag in kaart dat van Van de Velde medewerkers verwacht wordt bij het gebruik van de ICT middelen. Medewerkers zijn namelijk verantwoordelijk voor de verstrekte middelen, de bijhorende accessoires en de manier waarop hiermee wordt omgegaan.

## TOEPASSING

Onderhavige ICT-gedragscode is van toepassing op de medewerkers met een samenwerkingsovereenkomst met Van de Velde en diens dochtervennootschappen (hierna gezamenlijk “Van de Velde” genaamd). Onder dit begrip vallen zowel interne als externe medewerkers die voor Van de Velde werken.

Voor de werknemers van Van de Velde NV is de integrale policy inzake gebruik computer, internet & e-mail en telefoon terug te vinden in bijlage 7 van het arbeidsreglement. Deze policy blijft integraal van toepassing en heeft voorrang op deze ICT-gedragscode in geval van tegenstrijdigheid.

Indien u vragen heeft over de inhoud, kan u de personeelsdienst hiervan op de hoogte brengen door een e-mail te versturen naar people@vandevelde.eu.

# 2. HOOFDREGELS

Van de Velde beschouwt haar informatie- en technologieactiva als waardevolle bedrijfseigendommen. Ongepast gebruik of verspreiding van vertrouwelijke informatie kan Van de Velde en haar partners blootstellen aan risico’s. Daarom moet Van de Velde medewerkers bij het gebruik van data en apparatuur voldoen aan de toepasselijke wet- en regelgevingen en aanverwante gedragscodes van Van de Velde. Medewerkers moeten zich bewust blijven van hun professionele verantwoordelijkheden en verplichtingen die door ons bedrijf worden gecommuniceerd.

## GEDRAG TEN AANZIEN VAN VERSTREKTE APPARATUUR

Ter uitoefening van hun werkzaamheden, stelt Van de Velde apparatuur ter beschikking van haar medewerkers. Onder apparatuur verstaan we : laptop, GSM, desktop, tablet, printer, etc. Het uitgangspunt is dat medewerkers dit materiaal als een goed huisvader bedienen, om zodoende schade aan de appartatuur of de organisatie te beperken. De hoofdregels hieromtrent gelden als volgt :

- Tenzij uitdrukkelijk anders aangegeven (en op passende wijze gedocumenteerd in bijvoorbeeld een contract), blijven alle informatie- en technologieactiva eigendom van Van de Velde.
- Privégebruik van computer en internet wordt beperkt toegestaan. Af en toe moet je immers, net als met de telefoon, de mogelijkheid hebben om zaken te regelen die niet vanuit huis kunnen geregeld worden of niet kunnen wachten tot thuis. Twijfel je hierover, bespreek het dan met je leidinggevende.
- Telefoon is bedoeld voor zakelijk gebruik. Af en toe privégebruik is toegestaan, zolang het maar incidenteel is en op geen enkele manier het werk verstoort. Het gebruikmaken van commerciële betaalnummers die je niet uitdrukkelijk voor je werk nodig hebt, is niet toegestaan.
- Op laptops, desktops en tablets van Van de Velde mag enkel software worden geïnstalleerd door de ICT medewerkers en dit voor zakelijke doeleinden en beperkt prive-gebruik. Contacteer dus altijd de ICT afdeling om software te installeren of te verwijderen. Voor ICT medewerkers met admin rechten zal er een lijst ter

beschikking worden gesteld van software die zij mogen installeren op laptops, dekstops en tablets. Voor andere software dient er voorafgaand akkoord van de leidinggevende te worden bekomen.

- De ICT afdeling beschikt over een overzicht van toegelaten Cloud-oplossingen. De lijst is hier te vinden : https://howto.vandevelde.eu/display/VDVKB/Whitelist+%28cloud%29+applications.
- Laat steeds algemene voorwaarden checken door het legal departement vooraleer je deze aanvaardt.
- Het installeren van ongeoorloofde software is niet toegestaan. Onder “ongeoorloofde software” verstaan we o.m.:
    - Peer to Peer netwerken / download software (vb SpotNet, Bittorrent, PopcornTime)
    - Games
    - Software die voor privégebruik licentievrij is maar op een zakelijke werkplek wel licentieplichtig is
    - Software die privé is aangekocht maar waarvan de licentie-overeenkomst het niet toestaat om deze op zakelijke werkplekken te gebruiken
- Schade die aan Van de Velde wordt toegebracht waarbij de oorzaak ligt in het niet naleven van de punten hierboven, wordt direct toegerekend aan de medewerker.
- Apparatuur mag niet onbeheerd achtergelaten worden.
    - Indien niet anders mogelijk is, dient de apparatuur afgesloten en opgeborgen te worden in een afgesloten ruimte of kast.
    - Bij het verlaten van de werkplek voor beperkte tijd, vergrendelt de medewerker zijn scherm. (Dit kan bereikt worden door gelijktijdig Ctrl+Alt+Del in te toetsen en dan “Lock Workstation” aan te klikken (of door gelijktijdig de Windows-toets en “L” in te drukken).
    - Apparatuur wordt niet achtergelaten in de wagen
    - Bij verplaatsingen met het vliegtuig, worden de apparatuur en accessoires als handbagage meegenomen
    - Verlies of diefstal van de apparatuur dient onmiddellijk aan de ICT afdeling en de leidinggevende gemeld te worden.
- Wanneer apparatuur niet langer nodig is of defect raakt, moeten ze terugbezorgd worden aan de IT Helpdesk. In geen geval mogen medewerkers deze processen omzeilen, door bijvoorbeeld een apparaat naar een plaatselijke reparatiewerkplaats te brengen.

## GEDRAG TEN AANZIEN VAN INFORMATIE EN DATA

Medewerkers hebben toegang tot informatie, die al dan niet vertrouwelijk kan zijn. Indien informatie in verkeerde handen valt, kan dit tot schade leiden voor de organisatie. Medewerkers moeten zicht bewust zijn van de mogelijke risico’s nav het verliezen van informatie en dus adequaat handelen :

- Medewerkers gaan vertrouwelijk om met toegangsgegevens. Deze zijn strikt persoonlijk
    - Gebruikersnamen en wachtwoorden worden niet gedeeld
    - Gebruik sterke wachtwoorden en wijzig ze regelmatig. Schrijf ze niet op.
    - Gebruik wachtwoorden gebruikt in Van de Velde dienstverband niet voor andere systemen of apparatuur.
    - Bij het selecteren van wachtwoorden moeten medewerkers een complex wachtwoord maken dat zowel moeilijk te raden als gemakkelijk te onthouden is (zodat het nergens hoeft opgeschreven te worden). Wachtwoorden moeten minimaal acht (8) tekens bevatten en minsten drie (3) van de volgende vier (4) klassen bevatten: hoofdletters (bijv. A,B,C,…,Z), kleine letters (bijv. a,b,c,…,z), cijfers (bijv. 1, 2, …9), speciale tekens (bijv. ?, !, %, $, #, enz.). Indien dit niet wordt afgedwongen door de applicatie zelf, moeten wachtwoorden ook ten minste om de 90 dagen gewijzigd worden.
    - Wijzig je wachtwoord onmiddellijk indien delen niet vermeden kon worden (bijv. wanneer IT support nodig was).
- Medewerkers in beheersfuncties (helpdesk, systeem- of applicatiebeheerders) vragen nooit om de inloggegevens. In voorkomend geval, zal deze informatie niet verschaft worden door de medewerkers.
- Gebruik de door de organisatie verstrekte middelen voor het opslaan en communiceren van informatie en data :
    - Sla persoonlijke bestanden op in de Business OneDrive
    - Sla gedeelde bestanden op in :
        - Sharepoint (vb Teams)
        - Business OneDrive
        - Groups
        - OneDrive als je documenten wil delen met derde partijen

  - Back-ups gebeuren als volgt :
    - Alle Cloud-applicaties worden in real time ge-backupt
    - De Groups wordt drie maal per dag ge-backupt
  - Het gebruik van publieke diensten om Van de Velde- of consumenteninformatie te verwerken is niet toegestaan, vb :
    - WeTransfer
    - Dropbox
    - Google Drive
    - Persoonlijke webmail
    - WhatsApp
    - Siri
    - Google Translate
- Het gebruik van verwisselbare media (type niet-geëncrypteerde usb stick) om Van de Velde of consumentengegevens op te slaan wordt verboden.
- Werknemers zullen slechts uitzonderlijk persoonlijke informatie op hun apparatuur van Van de Velde bewaren. In voorkomend geval maak je een folder aan op de lokale C-drive. Deze informatie dient geïndividualiseerd te worden in een afzonderlijke folder waaruit opgemaakt kan worden dat deze “privé”-informatie bevat. Alle andere informatie blijft bedrijfsinformatie. De werknemer wordt geacht zelf te zorgen voor back-ups van deze informatie. Zodra de samenwerkingovereenkomst beëindigd wordt, zal het materiaal onmiddellijk aan Van de Velde worden terugbezorgd. De werknemer zal wel nog de mogelijkheid hebben om in aanwezigheid van een IT medewerker, een kopij te maken van deze privé folder.
- Medewerkers mogen geen services of apparaten instellen, activeren of gebruiken die bedoeld zijn om in het geheim details van vertrouwelijke vergaderingen of discussies op te nemen of te verzenden naar andere personen die niet rechtsreeks bij de vergadering betrokken zijn. Ongeoorloofd toezicht op personen is verboden. Opnames die zijn gemaakt met het doel notulen op te stellen of op een later tijdstip af te spelen voor geautoriseerde personen zijn echter wel toegestaan, maar het maken van dergelijke opnamen moet aan het begin van de procedure bekendgemaakt worden.
- Het is noodzakelijk dat beveiligingsincidenten onmiddellijk worden geïdentificeerd en gerapporteerd aan de IT Helpdesk, zodat de juiste corrigerende maatregelen zo snel mogelijk kunnen worden uitgevoerd. Een beveiligingsincident is een incident dat de vertrouwelijkheid, integriteit en beschikbaarheid van informatie of IT systemen van Van de Velde beïnvloed heeft of kan beïnvloeden. Bij beveiligingsincidenten met betrekking tot persoonsgegevens dient ook privacy@vandevelde.eu op de hoogte gesteld te worden.
  - Elke datalek met inbegrip van verkeerd geadresseerde e-mails, verlies van (persoonlijke) gegevens, intellectueel kapitaal, software of apparatuur, overdracht aan een ongeautoriseerde ontvanger, waaronder bijvoorbeeld informatie over laptops, smartphones, USB-apparaten en CD’s, documenten (zowel elektronisch als op papier), moet onmiddellijk worden gemeld;
  - Indien een medewerker van mening is dat zijn/haar inloggegevens werden aangetast of verloren, moet dit onmiddellijk bij de IT-helpdesk gemeld worden om de juist acties te ondernemen. Evenzo, in het geval dat een token of ander toegangsapparaat verloren geraakt, dient dit als incident behandeld te worden.
  - Elk computervirus of vermoeden van virus dient aan de IT Helpdesk gemeld te worden. Medewerkers zijn niet toegelaten het virus gerelateerde probleem zelf aan te pakken, maar dienen hulp te vragen aan de IT Helpdesk.
  - Ongepaste e-mails die de e-mailfiltercontroles hebben omzeild (bijv. phishing, social engineering) dienen ter nazicht aan de IT Helpdesk bezorgd te worden.
  - Elke overtreding van dit beleid moet onmiddellijk aan de IT Helpdesk gemeld worden.
  - Medewerkers dienen de IT Helpdesk op de hoogte te brengen indien een mobiel apparaat werd gestolen of verloren dat werd gebruikt voor zakelijke doeleinden.

## GEDRAG TEN AANZIEN VAN INTERNET

Het internet bevat een bron aan informatie maar kan ook leiden tot gevaren zoals vb spam, virussen, identiteitsdiefstal. Medewerkers dienen derhalve op een veilige en bewuste manier gebruik te maken van de internetfaciliteiten :

- Via het bedrijfsnetwerk is enkel internetverbinding toegestaan indien dit voor de uitoefening van de functie vereist is.

- Kortstondig gebruik voor persoonlijke doeleinden is toegestaan voor zover de dagelijkse werkzaamheden hier niet onder lijden. Onder “persoonlijke doeleinden” wordt niet verstaan, het gebruik van internet om :
    - Games te spelen / te downloaden
    - Te gokken of deel te nemen aan kansspelen
    - Niet werk-gerelateerde nieuwsgroepen of chatboxen te bezoeken
- Zorg ervoor dat je internet- en e-mailgebruik correct is, nooit aanstoot geeft en geen rechten van derden schendt of negeert. Gebruik internet dus op een manier die geen ongewenste publiciteit kan opleveren of andere nadelige effecten voor Van de Velde of andere partijen kan hebben. Het bekijken, downloaden, versturen of doorsturen van alles wat pornografisch, racistisch, discriminerend, beledigend of aanstootgevend is, is niet toegestaan. Als je dit soort e-mail ontvangt, maak de afzender dan duidelijk dat je dat niet wilt en bespreek met je leidinggevende of andere stappen noodzakelijk zijn.
- De ICT afdeling behoudt zich het recht voor om bepaalde internetsites te blokkeren. Indien toegang vereist is om bedrijfsdoeleinden, kan deze toegang op vraag gedeblokkeerd worden. Log hiervoor een Jira-ticket.
- Medewerkers die ervoor kiezen om persoonlijke informatie te bewaren (vb private keys, kredietkaartnummers) of gebruik maken van internet wallets, doen dit op eigen risico. Van de Velde is niet verantwoordelijk voor enig vorm van verlies van informatie of persoonlijke eigendommen als gevolg hiervan.

## GEDRAG TEN AANZIEN VAN E-MAIL

Van de Velde stelt medewerkers in staat om e-mail te gebruiken als communicatiemiddel voor het verzenden en ontvangen van informatie. Er schuilen echter ook risico’s in het gebruik van e-mail, zoals vb spam of phishing. Medewerkers dienen daarom te zorgen voor verantwoord e-mailgebruik :

- De werknemer zal bij de activatie van zijn e-mailadres, zijn e-mailhandtekening toevoegen in de banner. Hierin staat zijn naam, functietitel en telefoonnummer om zich te kunnen identificeren. De richtlijnen om de e-mailhandtekening op te laden, zijn beschikbaar op de Conversation Room (Files – Entity Van de Velde – Rubriek ICT)
- Het e-mailadres mag in principe alleen voor professionele doeleinden gebruikt worden.
- Het is niet toegestaan om Van de Velde documenten naar je privé-mailadres te sturen en vice-versa.
- Het is niet toegestaan om anonieme mails en/of ongevraagde mails (type spam) te versturen aan willekeurige medewerkers of een groep medewerkers uit het Van de Velde adresboek.
    - E-mails mogen niet worden ondertekend met een andere naam zonder toestemming van de afzender
    - Medewerkers doen niet mee aan kettingmails
- E-mails van onbekende afzenders worden zorgvuldig beoordeeld. Medewerkers beoordelen de authenticiteit van de mail aandachtig, zo ook bij het openen van bijlagen en klikken op links.
- Bij langdurige afwezigheid (vb vakantie) stelt de werknemer een out-of-office bericht in om de zenders te informeren van de afwezigheid. Bij onvoorziene afwezigheid (vb. overmacht of ziekte) stemt de medewerker er tevens mee in dat dergelijke out of office bericht door de ICT afdeling ingesteld kan worden
- Generieke mailboxen worden binnen de desbetreffende departementen beheerd.
- Bij beëindiging van de samenwerkingsovereenkomst zijn volgende bepalingen van toepassing:
    ° ten laatste op het moment van effectieve beëindiging van de tewerkstelling zal het e-mail account van de betrokken werknemer geblokkeerd worden en er zal er door de ICT afdeling voorzien worden in een automatisch bericht waarin de geadresseerde wordt geïnformeerd dat de persoon die hij probeerde te contacteren, de organisatie heeft verlaten;
    ° voorafgaand aan het deactiveren van de mailbox zal de betrokken werknemer – in aanwezigheid van een andere Van de Velde medewerker aangeduid door de ICT afdeling- de mogelijkheid krijgen om zijn mails te klasseren en eventuele privé mails door te sturen naar zijn privé e-mailadres
    ° binnen een maand na het einde van de effectieve tewerkstelling zal de mailbox en het automatisch bericht verwijderd worden. De werknemer stemt er mee in dat gedurende die maand de werkgever toegang zal hebben tot de mailbox en mails kan recupereren en dit teneinde de onderneming in staat te stellen de voortzetting van de taken mogelijk te maken en de goede werking van de onderneming te verzekeren.
- Waar nodig moeten e-mailbijlagen afzonderlijk worden gecodeerd. In die gevallen moeten bijlagen eerst worden gecodeerd met behulp van een goedgekeurd product (bijv. WinZip) voordat het bestand als bijlage aan het e-mailbericht wordt toegevoegd. Bij het verzenden van de gecodeerde bestandsbijlagen moet de afzender ook het wachtwoord opgeven. Om de veiligheid van de gegevens te waarborgen, moet het wachtwoord buitenom vertrekt worden bijv. dor de ontvanger rechtsreeks te bellen.

- Indien informatie (met name persoonsgegevens) werden verstuurd naar een onbedoelde ontvanger, dient dit meteen gerapporteerd te worden aan de IT Helpdesk zodat de nodige stappen ondernomen kunnen worden.

## GEDRAG TEN AANZIEN VAN SOCIALE MEDIA

De grens tussen privé en zakelijk is op sociale media niet altijd te onderscheiden. Social media berichten met een link naar Van de Velde hebben een invloed op het beeld dat medewerkers, klanten en andere doelgroepen van Van de Velde hebben. Het uitgangspunt is daarom dat medewerkers zich professioneel en respectvol opstellen op sociale media :

- Breng de naam van de organisatie niet in discrediet. Sociale media hebben een groot bereik, en derden maken geen onderscheid tussen werk en privé. Medewerkers van Van de Velde worden daarom geacht hun gezond verstand te gebruiken bij het plaatsen van berichten op sociale media.
- Bij het registreren, inschrijven of online posten, mogen medewerkers hun Van de Velde e-mailadres of andere Van de Velde gegevens niet gebruiken, tenzij noodzakelijk voor zakelijke of professionele doeleinden.
- Gebruik niet de naam of het logo van de organisatie in je profielnaam of -foto. Deze worden enkel gebruikt in de offiële communicatiekanalen van Van de Velde op sociale media. Aangeven dat je bij Van de Velde werkt mag wel, dat wordt zelfs aangemoedigd, maar medewerkers dienen er zich bewust van te zijn dat hetgeen wordt opgeschreven, ook van invloed is op de organisatie.
- Het is niet toegestaan om onder de naam van Van de Velde te reageren op juridische of / en politiek getinte discussies. Het respect voor andere mensen, culturen en waarden dient te worden bewaard.
- Medewerkers mogen van gedachten wisselen over ideeën, maar nooit over personen. Uitlatingen dienen te worden onderbouwd met feiten, cijfers, bronnen.
- Het is niet toegestaan om interne en / of vertrouwelijke informatie op sociale media te plaatsen. Indien bepaalde nieuwsberichten of aankondigingen worden gedaan over de organisatie of onderdelen van de organisatie, wordt dit enkel via de officiële kanalen gedaan.

## LAPTOP POLICY

Deze Laptop policy is van toepassing voor alle medewerkers voor wie een laptop en/of toebehoren zoals muis, scherm, toetsenbord, oplader etc. (hierna: '**Laptop**') door Van de Velde wordt voorzien op basis van de functieomschrijving. Onverminderd het hierna gestelde, gaat de medewerker ermee akkoord dat hij of zij nooit enig eigendomsrecht kan doen gelden op de hem of haar toegekende Laptop en dat zijn of haar gebruiksrecht beperkt is volgens de hierna omschreven modaliteiten van de Laptop policy. In geval van een geschil of bij geschillen die niet zijn voorzien in deze policy, beslist het Head of IT.

- Goedkeuring en aanvraag: Het initieel ter beschikking stellen van een Laptop wordt goedgekeurd door het Management Team. De aanvraag wordt door HR aan IT doorgegeven die de Laptop en de aansluiting ervan voorziet. De medewerker kan de Laptop in ontvangst nemen na ondertekening van een ontvangstbewijs.

- Schade, verlies of diefstal
  - **Eerste voorval**:
    - Bij onherstelbare schade, verlies of diefstal van de Laptop betaalt de medewerker een franchise van maximum 100€.
    - Bij herstelbare schade betaalt de medewerker 50% van de schadefactuur, met een maximum van 100€.
  - **Tweede of hierop volgende voorval**: In geval van (on)herstelbare schade/ verlies/ diefstal van de Laptop, wordt het bedrag van de herstelfactuur of aankoopfactuur van de nieuwe Laptop ter vervanging volledig betaald door de medewerker. De teller wordt gereset 2 jaar na het eerste voorval.
  - **Diefstel in onze bedrijfsgebouwen**: De Laptop dient 's avonds mee naar huis genomen worden, ofwel in een afgesloten kast opgeborgen. Indien het toestel uit de kast wordt gestolen, dient de medewerker niets te betalen.
  - **Overmacht**: HR & IT kunnen in samenspraak beslissen om deze kosten toch op het bedrijf te nemen indien het blijkt door overmacht te zijn (bijvoorbeeld: technisch defect).

- Vervanging
  1. Ten gevolge van schade, verlies of diefstal

In geval een Laptop wordt vervangen ten gevolge van schade, verlies of diefstal van een eerder voorziene Laptop, zal IT hiervoor een Laptop voorzien die binnen het gewoonlijke budget valt zoals bepaald door het Head of IT.

2. Upgrade
In geval een speciale aanvraag wordt gedaan om een duurdere Laptop of PC te ontvangen, die niet binnen het gewoonlijke budget valt zoals bepaald door het Head of IT, dan zal dit goedgekeurd moeten worden door het Head of IT.

- Goed huisvaderschap
De gebruiker/medewerker zal de laptop als een goede huisvader gebruiken. Dit betekent onder andere (niet limitatieve lijst):
  - Hij gaat zorgvuldig om met de Laptop.
  - Hij engageert zich om bij elke schade, verlies of diefstal onmiddellijk zijn rechtstreekse leidinggevende alsook IT en HR Van de Velde op de hoogte te brengen.
  - Het uitlenen van de Laptop aan derden is verboden.

  Het gebruik van de Laptop kan onmiddellijk verboden worden. De werkgever heeft altijd het recht de teruggave van de Laptop te eisen. Een teruggave van de Laptop is vereist, onder andere, bij misbruik van de Laptop door de medewerker (vb. stalking, overdreven privé gebruik tijdens de werkuren, …)

- Medewerker uit dienst
Wanneer een medewerker uit dienst gaat, wordt de Laptop opnieuw ingeleverd bij Van de Velde.

- Einde gebruik en vervanging
Het gebruiksrecht over de Laptop kan beëindigd worden, wanneer een van de volgende situaties zich voordoet:
1. schorsing van de arbeidsovereenkomst langer dan 1 maand
2. onzorgvuldig gebruik/misbruik van de Laptop (in strijd met de letter en/of de geest van deze policy)
3. gewijzigde functie of functie-inhoud, die niet in aanmerking komt voor een Laptop

  Bij beëindiging van het gebruiksrecht zal de gebruiker de Laptop terugbezorgen aan IT. Een Laptop kan vervangen worden op initiatief van IT.

# 3. NALEVING, CONTROLES EN SANCTIES

**3.1 Voor de werknemers van Van de Velde nv**

Voor de werknemers van Van de Velde nv kan voor dit hoofdstuk integraal verwezen worden naar punt 3 en 4 van bijlage 7 aan het Arbeidsreglement.

**3.2 Voor de andere medewerkers op wie dit beleid van toepassing is**

Indien een werknemer of een groep van werknemers ervan wordt verdacht om de ICT-richtlijnen niet te respecteren, kan gedurende een vastgestelde periode op individuele basis een gerichte controle plaatsvinden. Hiervoor is voorafgaande toestemming nodig, die hierna wordt omschreven. De controle kan zich uitstrekken tot gegevens die betrekking hebben op de periode die gelegen is voor het tijdstip van de verkregen toestemming.

## CONTROLE

### ALGEMEEN

Om de goede werking van de e-mail en internet systemen van de organisatie te verzekeren, houdt de ICT afdeling een logboek bij van verzonden en ontvangen e-mails, inclusief het onderwerp, exclusief de inhoud ervan. De volgende richtlijnen worden hierbij gehanteerd:

- on-line storage in de Cloud
- off-line storage op de hard disc van de gebruiker

Enkel medewerkers van de IT afdeling hebben toegang tot deze systemen, in zoverre dit tot hun takenpakket behoort. Deze medewerker zijn gehouden aan de regels rond vertrouwelijkheid van persoonlijke data.

### CONTROLE OP GEDRAG TEN AANZIEN VAN VERSTREKTE APPARATUUR

Voor de controle op individuele basis van geïnstalleerde software op apparatuur, moet voorafgaand toestemming verkregen worden van het hoofd van de IT-afdeling en HR Director, met uitzondering van controles op de automatische detectie van ongewenste of niet-gelicenseerde software op werkplekken die schade kunnen toebrengen aan Van de Velde. Hierover mag de medewerker direct worden aangesproken en verzocht deze software te verwijderen.

### CONTROLE OP GEDRAG TEN AANZIEN VAN INFORMATIE EN DATA

Voor de controle op individuele basis van de omgang met informatie moet voorafgaand toestemming verkregen worden van het hoofd van de IT-afdeling en de HR Director.

### CONTROLE OP GEDRAG TEN AANZIEN VAN INTERNET

Van de Velde zal, tenzij er aanleiding voor is, geen controle uitvoeren op internetgebruik. Indien er vermoedens op misbruik bestaan, zal er gerichte controle plaatsvinden door de IT afdeling. Voor de controle op individuele basis van internetgebruik, meot voorafgaand toestemming verkregen worden van het hoofd van de IT-afdeling en de HR Director.

### CONTROLE OP GEDRAG TEN AANZIEN VAN E-MAIL

Van de Velde zal de inhoud van e-mailberichten niet lezen. Eveneens zullen persoonsgegevens mbt het aantal e-mails, e-mailadressen en andere data hieromtrent niet gecontroleerd worden. Dit neemt niet weg dat er vanwege een zwaarwegende reden controles kunnen plaatsvinden op incidentele basis op aantal mails, mailadressen of andere data. Hiervoor is een voorafgaande toestemming van het hoofd van de IT-afdeling en de HR Director vereist.

### CONTROLE OP GEDRAG TEN AANZIEN VAN SOCIALE MEDIA

Van de Velde zal de medewerkers niet monitoren en controleren op het gebruik van sociale media, ook niet onder de werktijd of op de apparatuur van de organisatie. Mocht wangedrag toch blijken, ook indien dit door een derde aan Van de Velde wordt gemeld, mag Van de Velde op basis van deze informatie de medewerker hierop aanspreken.

### TOEGANKELIJKHEID

Indien controles worden uitgevoerd door de ICT afdeling, zal de medewerker de nodige informatie en resources aan de werkgever ter beschikking stellen (vb access codes, decryptie sleutels, etc.) om de check te kunnen doen.

## SANCTIES

Een medewerker die de regels overtreedt,  moet weten dat Van de Velde dit serieus opneemt.  Het kan leiden tot diverse sancties, variërend van een waarschuwing tot ontslag om dringende reden en dit afhankelijk van de ernst van de situatie.

# 4. MONITORING

Compliance met deze ICT-gedragscode wordt opgevolgd door de HR en ICT-afdeling. Medewerkers kunnen dit department contacteren met vragen, opmerkingen of / of suggesties.