Gedragscode gebruik bedrijfsmiddelen ict en internet Winkler Prins 2019

Versie februari 2019

Winkler Prins
openbare school voor voortgezet onderwijs

Inhoudsopgave

1. Inleiding

Het gebruik van internet, computernetwerk en e-mail is voor alle medewerkers van de school noodzakelijk om de werkzaamheden te kunnen verrichten. Bij deze werkzaamheden wordt gebruik gemaakt van veel gegevens, waaronder persoonsgegevens. De (ict)-faciliteiten en de verschillende gegevens worden in dit document **bedrijfsmiddelen** genoemd.
Onder bedrijfsmiddelen worden in ieder geval verstaan:

- Hardware: *pc, laptop, tablet, telefoon, hardware token (tag).*
- Software (of -systemen): *alle applicaties voor het uitvoeren van de werkzaamheden, zoals de school e-mailomgeving, Microsoft Office, administratiesystemen en (online) digitaal lesmateriaal, maar ook apps op (mobiele) devices.*
- Informatie en (persoons)gegevens: *rapportages, leerlingdossiers, gegevens in e-mails. Hierbij vraagt de verwerking van persoonsgegevens vanuit de privacywetgeving extra maatregelen.*
- Internetgebruik: *het bezoeken van het World Wide Web, het gebruik van e-mail en diensten als FTP (File Transfer Protocol zoals Wetransfer, Dropbox), maar ook sociale media zoals Facebook, LinkedIn, Instagram en Twitter.*

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers van *Stichting Winkler Prins* wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor de school uit te voeren.

De afspraken in dit document gelden voor alle locaties van waaruit (school)werkzaamheden worden verricht en voor alle devices waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij *Stichting Winkler Prins,* ook voor uitzendkrachten, tijdelijke werknemers, e.d..
Deze gedragscode is opgesteld aan de hand van de handreiking van Kennisnet, m.m.v. de VO-raad.

1.1 Uitgangspunten gedragscode

Deze gedragscode legt regels vast voor het gebruik van de bedrijfsmiddelen door medewerkers en over de controle op de naleving hiervan.
Het doel van deze gedragscode is om de normen en uitgangspunten vast te leggen ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
- het tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
- de bescherming van privacygevoelige informatie waaronder persoonsgegevens van het schoolbestuur, haar medewerkers, leerlingen en hun ouders en daarmee het beschermen van de privacy en veiligheid van alle betrokkenen;
- de bescherming van vertrouwelijke informatie van het schoolbestuur, haar medewerkers, leerlingen en hun ouders;
- het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen;
- de bescherming van de intellectuele eigendomsrechten van het schoolbestuur en derden;
- het voorkomen van negatieve publiciteit;
- kosten- en capaciteitsbeheersing.

De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. Stichting Winkler Prins zal dan ook de controle en handhaving van deze regels conform de privacywetgeving en het algemene arbeidsrechtelijk kader uitvoeren. Hierbij is het uitgangspunt een goede balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers op de werkplek. Gegevens worden alleen verzameld en gebruikt voor deze doelen. In het bijzonder zal het bestuur de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang.

1.2 Eigen verantwoordelijkheid en privégebruik

Het gebruik van door Stichting Winkler Prins verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle devices die voor schoolwerk worden gebruikt (inclusief eigen devices) worden niet uitgeleend of aan anderen ter beschikking gesteld zonder aanvullende (beveiligings)maatregelen.

1.3 Verschillende soorten gegevens

Stichting Winkler Prins is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens.
Stichting Winkler Prins onderscheidt drie typen gegevens:

- **Openbare gegevens**; dit zijn gegevens die juist voor publicatie bedoeld zijn.
- **Interne gegevens**; dit zijn gegevens die alleen voor gebruik en verwerking binnen Stichting Winkler Prins bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- **Vertrouwelijke gegevens**; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen Stichting Winkler Prins toegankelijk zijn. Denk hierbij aan (bijzondere) persoonsgegevens, personeelsgegevens of aanbestedingsgegevens.

Persoonsgegevens verdienen bijzondere aandacht. Dit zijn gegevens die een persoon betreffen én waardoor een persoon geïdentificeerd of identificeerbaar is. Denk hierbij aan naamgegevens, e-mailadressen, maar ook telefoonnummers van zowel collega's als leerlingen en ouders van leerlingen.

De privacywetgeving verplicht elk individu om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat Stichting Winkler Prins schriftelijk afspraken maakt met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk).
Stichting Winkler Prins heeft een Functionaris voor gegevensbescherming (FG) aangesteld. Deze communiceert intern de gedragsregels die horen bij het verwerken van persoonsgegevens. Persoonsgegevens moeten altijd met uiterste zorgvuldigheid verwerkt en gedeeld worden.

Als persoonsgegevens toegankelijk en/of inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot deze gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en Stichting Winkler Prins.
Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt Stichting Winkler Prins afspraken over:
- de verwerking en verspreiding van vertrouwelijke data en persoonsgegevens. Er worden niet meer gegevens verwerkt dan noodzakelijk om het doel te bereiken;
- de uitwisseling van gegevens, waarbij aan de ontvanger wordt aangegeven wat de ontvanger wel of niet mag doen met de gegevens;
- opslag en verspreiding van gegevens, waarbij alléén gebruik gemaakt wordt van door Stichting Winkler Prins goedgekeurde bedrijfsmiddelen.

Van medewerkers van Stichting Winkler Prins en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bijvoorbeeld personeelsdossiers, vertrouwelijke enquêtegegevens, zorgdossiers et cetera, wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. Dat zij de privacywetgeving hanteren en op geen enkele wijze informatie, waarvan redelijkerwijze kan worden aangenomen dat deze vertrouwelijk of privacygevoelig is, zonder toestemming van betrokkene of leidinggevende te gebruiken en/of naar buiten te brengen.

2. Gedragscode

In deze gedragscode voor verantwoord gebruik van bedrijfsmiddelen geeft Stichting Winkler Prins aan wat de afspraken zijn met betrekking tot verschillende onderwerpen rondom het gebruik van bedrijfsmiddelen en wat dit voor de medewerkers in de dagelijkse praktijk betekent.

2.1 Algemene normen

Iedere medewerker voldoet aan de volgende algemene normen voor 'zorgvuldigheid' (niet uitputtend):
- Ga zorgvuldig om met persoonsgegevens.
- Voorkom het lekken van interne en vertrouwelijke informatie.
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen.
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild.
- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering aan de functionaris IBP door het sturen van een e-mail aan security@winklerprins.nl (zie hiervoor ook het Protocol informatiebeveiligingsincidenten en datalekken Winkler Prins).

2.2 Computergebruik

Voor het uitoefenen van de werkzaamheden stelt Stichting Winkler Prins aan de medewerker computer- en netwerkfaciliteiten (ict-bedrijfsmiddelen) ter beschikking. Het gebruik van deze ict-bedrijfsmiddelen is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:
- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.

- Weet welke gegevens er mogen worden gebruikt (mag iedereen het zien?) en welke ict-voorzieningen kunnen worden ingezet (is het veilig genoeg?) bij het verrichten van de verschillende schoolwerkzaamheden.
- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op. Opslaan van gegevens in public Cloud omgevingen, zoals een persoonlijke dropbox, is niet toegestaan.
- Versleutel alle gegevens met betrekking tot Stichting Winkler Prins, indien deze gegevens, om welke reden dan ook, elders opgeslagen worden (denk hierbij ook aan een usb-stick).
- Wachtwoorden zijn persoonlijk. Deel wachtwoorden nooit, ook niet incidenteel.
- Sluit na gebruik de computer af of log uit.
- Meld storingen van beheerde werkplekken (computer of laptop) bij de ict-afdeling via de workflow digitaal op Mijn Winkler Prins.
- Het ge- en verbruik van materialen (bijvoorbeeld printen) staat alleen ten dienste van het leerproces dan wel de uit te voeren werkzaamheden.
- Het is niet toegestaan al dan niet eigen apparatuur of bekabeling aan of los te koppelen van het schoolnetwerk.
- Het is niet toegestaan door de school aangebrachte beveiligingen in het netwerk of aan bestanden te omzeilen, teniet te doen, of gegevens of programma's te wissen of standaardinstellingen te wijzigen.

2.3 Werkplek

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen waartoe zij geen rechten hebben en/of laat gegevens niet (onbedoeld) lekken. Als aanvullende regels op computergebruik gelden voor de werkplek de volgende clean desk en clear screen regels:

- Vergrendel bij het tijdelijk verlaten van de werkplek de pc (windowstoets+L).
- Verwijder interne en vertrouwelijke documenten van het bureau bij het voor langere tijd verlaten van de werkplek (denk hieraan bij het bijwonen van een vergadering).
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via een beamer) mee kan kijken. Sluit het e-mail programma af en zorg voor een opgeruimd digitaal bureaublad.
- Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan.
- Verwijder overbodig geworden papieren documenten met persoonsgegevens erop altijd door gebruikmaking van de papiercontainer voor vernietiging vertrouwelijke informatie.

Als persoonsgegevens toegankelijk/inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot die gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Beveiligingsincidenten en mogelijke datalekken moeten gemeld worden volgens de Protocol informatiebeveiligingsincidenten en datalekken Winkler Prins.

2.4 Bring Your Own Device (BYOD)

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor Stichting Winkler Prins worden uitgevoerd. Stichting Winkler Prins is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school.

Voor het gebruik van eigen devices ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

- Beveilig het device met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode die langer is dan 4 tekens.
- Vergrendel het device bij het verlaten van de werkplek (windowstoets+L).
- Het is niet toegestaan persoonsgegevens van Stichting Winkler Prins op het eigen device op te slaan.
- Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot Stichting Winkler Prins als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden (denk hierbij aan het eigen device of usb-stick).
- Scheid (versleutelde) gegevens, anders dan persoonsgegevens, van Stichting Winkler Prins en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen device.
- Houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks).
- Neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het periodiek (minimaal maandelijks) scannen van het device.

Stichting Winkler Prins mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van Stichting Winkler Prins moet de medewerker zelf aantonen dat de bovenstaande maatregelen worden toegepast.

2.5 Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal is niet meer weg te denken bij Stichting Winkler Prins. Dit lesmateriaal staat steeds meer online waarbij steeds vaker persoonsgegevens worden uitgewisseld. De privacywetgeving eist dat elke organisatie vooraf aan het gebruik van dergelijk materiaal bekijkt wat de invloed ervan is op de privacy, dit kan specifieke maatregelen tot gevolg hebben.
De onderstaande regels gelden voor installatie en gebruik van software en (online)digitaal lesmateriaal:

- Installeren van software wordt bij Stichting Winkler Prins alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen.
- Bij het gebruik van online software, apps en digitaal lesmateriaal, wordt gekeken of er persoonsgegevens bij verwerkt worden.
- Een verwerkersovereenkomst wordt afgesloten met elke leverancier van (online)software, die in opdracht van Stichting Winkler Prins persoonsgegevens verwerkt. Dit dient vooraf te worden afgestemd met de leverancier.
- Verwerkersovereenkomsten worden gesloten op basis van het meest recente model verwerkersovereenkomst die hoort bij het convenant Digitale onderwijsmiddelen en privacy (medio mei 2018: versie 3.0; www.privacyconvenant.nl).
- De verwerkingsverantwoordelijke van de Stichting Winkler Prins (de bestuurder) is de enige functionaris die de verwerkersovereenkomsten aangaat (= ondertekent).
- Aanvragen van digitaal lesmateriaal en/of andere software bij Stichting Winkler Prins gaat via de coördinator leermiddelen volgens de jaarlijks afgesproken aanvraagprocedure. Hierbij moet rekening gehouden worden met eventuele wettelijk verplichte aanvullende privacy- en/of beveiligingsmaatregelen.

2.6 Gebruik van e-mail

Stichting Winkler Prins stelt een e-mailsysteem en een bijbehorende mailbox aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik van e-mailfaciliteiten is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Gebruik het school e-mail adres alleen voor school gerelateerde zaken.
- Gebruik voor privé e-mail een eigen privé e-mailadres via een externe webmaildienst. (bijvoorbeeld webmail van Gmail, Hotmail of een andere provider).
- Ontvangen van privémail op het school e-mailadres is in beperkte mate toegestaan.
- Het is niet toegestaan e-mail te gebruiken voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of voor berichten die kunnen aanzetten tot haat en geweld.
- Synchroniseert een medewerker de school e-mail met eigen devices (tablet, telefoon) dan kan Stichting Winkler Prins, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het device gewist worden.

2.7 Gebruik van internet

Stichting Winkler Prins stelt het gebruik van internet en de bijbehorende faciliteiten aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik hiervan is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Beperkt persoonlijk gebruik is toegestaan, mits dit
  - niet storend is voor de dagelijkse werkzaamheden
  - niet voor commerciële doeleinden is en
  - geen verboden gebruik oplevert.
- Het is niet toegestaan om
  - op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten
  - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron
  - onder lestijd internettoegang te gebruiken voor privédoeleinden
  - deel te nemen aan kansspelen.
- Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale netwerken en andere vergelijkbare communicatienetwerken over alle aan school verbonden betrokkenen en activiteiten. Dit geldt in het

bijzonder ook voor internetgebruik buiten het schoolnetwerk met betrekking tot aan de school verbonden betrokkenen en activiteiten.

2.8 Veilig online

We brengen met z'n allen steeds meer tijd online door. Hierbij worden steeds meer mobiele devices gebruikt. Menselijk (online)handelen staat veelal aan de basis van een datalek.
Stichting Winkler Prins verwacht van medewerkers dat zij:

- het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken) en websites;
- bij het verwerken van persoonsgegevens alléén gebruik maken van bekende én beveiligde draadloze netwerken;
- weten wat malware is, het kunnen herkennen en weten hoe te handelen;
- terughoudend zijn met het online achterlaten van gegevens met betrekking tot Stichting Winkler Prins;
- controleren of er daadwerkelijk van een bekend én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes.

2.9 Sociale media

Sociale media is een verzamelnaam voor alle internettoepassingen die het mogelijk maken om informatie met elkaar te delen op een eenvoudige en vaak leuke manier. Het gaat hierbij niet alleen om informatie in de vorm van tekst (nieuws, artikelen). Ook geluid (podcasts, muziek) en beeld (fotografie, video) worden gedeeld via social media (Instagram, YouTube, Facebook, Twitter enz). De essentie van sociale media is dat iemand er informatie deelt over zichzelf, over anderen of over een bepaald onderwerp.
Voor gebruik van sociale media geldt als uitgangspunt dat het digitale gedrag op sociale media niet afwijkt van het real life gedrag binnen de school. Medewerkers zijn altijd de vertegenwoordiger van Stichting Winkler Prins ook als zij online een privémening verkondigen.
De afspraken rondom social media zijn door Stichting Winkler Prins vastgelegd in een apart social mediaprotocol.

2.10 Gebruik beeld- en geluidsmateriaal

Het gebruiken van beeld- en geluidsmateriaal, het delen van foto's, video's en geluidsfragmenten van leerlingen door medewerkers vallend onder Stichting Winkler Prins mag alleen als daar vooraf toestemming voor gegeven is door ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder dan 16 jaar is. Zonder deze toestemming mogen geen foto's, video's en geluidsfragmenten van leerlingen gebruikt worden.

- Stichting Winkler Prins verwijst hierbij naar de 'Publicatie beeldmateriaal Winkler Prins' voor het gebruik en toestemming van beeldmateriaal.
- Voor de afspraken rondom het delen van beeld- en geluidsmateriaal via sociale media gelden de richtlijnen die genoemd worden bij het gebruik van sociale media.

2.11 Wachtwoorden en pincodes

Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en devices (pc, laptop, telefoon) begint met een goed wachtwoord. Een lang wachtwoord of een 'wachtzin' is beter dan een kort, complex wachtwoord. Voor het gebruik van wachtwoorden gelden onderstaande afspraken:

- Wachtwoorden moeten minimaal 8 tekens bevatten, met minstens drie van de volgende vier elementen: kleine letter, hoofdletter, cijfer of speciaal teken (!@#$%^&*(). Een pragmatische en effectieve oplossing voor een goed wachtwoord, is het gebruik van een wachtwoordzin. Een wachtwoordzin is beter te onthouden dan een lange letter-/woordcombinatie. Maak bijvoorbeeld een goed te onthouden zin als 'Ik ga 1 keer per jaar naar Ameland' en verwerk daar ook een hoofdletter, cijfer of leesteken in: Ikga1xperjaarnaar@meland. Indien het aantal tekens voor een wachtwoord beperkt is verkort de wachtzijn dan: Ig1xpjn@
- Pincodes (op telefoon of tablet) moeten langer zijn dan 4 tekens.
- Wachtwoorden moeten volgens de afspraken binnen Stichting Winkler Prins op aangegeven tijden vervangen worden.
- Gebruik niet voor elk systeem hetzelfde wachtwoord.
- Wachtwoorden zijn persoonlijk. Deel wachtwoorden nooit, ook niet incidenteel.

2.12 Meldplicht Datalekken
Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens het Protocol informatiebeveiligingsincidenten en datalekken Winkler Prins.

3. Controle gebruik bedrijfsmiddelen
Stichting Winkler Prins handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:
- De Grondwet,
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Wet Medezeggenschap Onderwijs (WMO)
- Burgerlijk Wetboek (BW)
- Wetboek van Strafrecht
- Cao VO.

Stichting Winkler Prins zal bij controle rondom het gebruik van bedrijfsmiddelen op basis van deze gedragscode uitgaan van de juiste balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers.

3.1 Voorwaarden voor controle
- Controle van persoonsgegevens met betrekking tot gebruik van bedrijfsmiddelen vindt slechts plaats in het kader van handhaving van de doelen van deze gedragscode.
- Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
- Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode, in opdracht van Stichting Winkler Prins gerichte controle plaatsvinden.
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts indien er sprake is van gerechtvaardigd belang, kan in opdracht van Stichting Winkler Prins, controle op de inhoud plaatsvinden.
- Verboden e-mail- en internetgebruik wordt zo veel mogelijk onmogelijk gemaakt.
- Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken medewerker besproken. Stichting Winkler Prins zal de medewerker op verzoek inzage verschaffen in de gegevens over het eigen gebruik. De medewerker wordt gewezen op de consequenties wanneer niet wordt gestopt met het ongeoorloofd gebruik.
- E-mailberichten van leden van de MR onderling, van vertrouwenspersonen, bedrijfsartsen, de Functionaris voor de Gegevensbescherming en van een ieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden niet gecontroleerd, tenzij er sprake is van gerechtvaardigd belang en het doel van de controle niet op een andere minder vergaande manier kan worden bereikt.

3.2 Uitvoering van de controle
- De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering.
- De controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering onder verantwoordelijkheid van de stafdirecteur facilitair/ICT. Verdachte berichten worden apart gezet voor nader onderzoek. Deze gegevens worden maximaal zeven dagen bewaard.
- De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens.
- De controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.
- De afdeling ict, de systeembeheerder(s) zijn aan geheimhouding gebonden als men om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.
- Door Stichting Winkler Prins worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- Door Stichting Winkler Prins worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

3.3 Disciplinaire maatregelen

Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het bestuur van Stichting Winkler Prins, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen. Hieronder vallen o.a. een waarschuwing/berisping, schadevergoeding, aangifte bij de politie, overplaatsing, schorsing en/of beëindiging van de aanstelling.
Medewerkers die zich niet aan deze gedragscode houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken. Zij krijgen daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. Medewerker en leidinggevende maken dan afspraken voor de toekomst en bepalen de mogelijke maatregelen bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in deze gedragscode bepaalde. Ook kan de toegang tot e-mail of internet worden beperkt of geheel worden afgesloten. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens worden getroffen, zoals een constatering van een automatisch filter of blokkade. Er worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

3.4 Bezwaar en beroep

Als de medewerker het niet eens is met de (voorgenomen) disciplinaire maatregel, dan kan daar in een aantal gevallen bezwaar en/of beroep tegen worden ingesteld. Dit is geregeld in de Bezwarenprocedure Winkler Prins en de van toepassing zijnde CAO.

4. Tot slot

1. De ‘Gedragscode gebruik bedrijfsmiddelen ict en internet Winkler Prins 2019’ is vastgesteld door het bevoegd gezag van Winkler Prins op 20 juni 2019 nadat de medezeggenschapsraad van Winkler Prins heeft ingestemd met de gedragscode in de vergadering van 19 juni 2019.
2. Het bevoegd gezag stelt alle belanghebbenden op de hoogte van deze gedragscode.
3. De gedragscode is via www.winklerprins.nl te downloaden of op verzoek bij een lid van het managementteam van de school op te vragen.
4. De gedragscode kan door het bevoegd gezag worden gewijzigd of ingetrokken, met inachtneming van de geldende bepalingen.