Gedragscode voor verantwoord gebruik van ICT middelen door medewerkers
Stichting Achterhoek VO

Instemming GMR: 27 september 2022

Vaststelling bestuur: 3 oktober 2022

Inwerkingtreding: 3 oktober 2022

Bron

Deze gedragscode is opgesteld op basis van de ‘Handreiking verantwoord gebruik van bedrijfsmiddelen’ (11 april 2019) van Kennisnet. De code is, mede naar aanleiding van opmerkingen van de Beleidsgroep ICT, aangepast voor Achterhoek VO.

Inhoud

1 Doel

Deze gedragscode voor verantwoord gebruik van ICT-middelen voor medewerkers bevat afspraken over de wijze waarop Achterhoek VO omgaat met het gebruik van e-mail, intranet, internet, Microsoft 365 apps, etc. Deze gedragscode komt in plaats van het verouderde Internet- en e-mailprotocol versie 1.3. uit 2018. Voor de werkgever geeft deze gedragscode de mogelijkheid om onrechtmatig gebruik op te sporen, ongewenst gebruik terug te dringen en waar nodig sancties bij overtreding van de opgestelde regels op te leggen. Voor de medewerker geeft deze gedragscode duidelijkheid over de regels met betrekking tot het gebruik van ICT-middelen en de controlemogelijkheden op het gebruik ervan door Achterhoek VO. Voor de medewerker en werkgever biedt deze gedragscode een kader waarin duidelijke afspraken staan over het gebruik van de mogelijkheden waarbij de privacy van zowel individu als organisatie wordt gewaarborgd.

2 Inleiding

Het gebruik van e-mail, intranet, internet, Microsoft 365 apps en vele andere ICT-toepassingen is voor alle medewerkers van Achterhoek VO 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 van Achterhoek VO worden in dit document **bedrijfsmiddelen** genoemd. Onder bedrijfsmiddelen worden in ieder geval verstaan:

- Hardware: *pc, laptop, tablet, (netwerk)printers hardware token (tag).*
- Software (of -systemen): *alle applicaties voor het uitvoeren van de werkzaamheden, zoals de e-mailomgeving, Microsoft Office, administratiesystemen en (online)digitaal lesmateriaal maar ook apps op (mobiele) apparaten.*
- Informatie en (persoons)gegevens: *rapportages, leerling dossiers, 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 het gebruik van 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 Achterhoek VO wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor Achterhoek VO uit te voeren.

De afspraken in dit document gelden voor alle scholen en locaties van Achterhoek VO van waaruit (school)werkzaamheden worden verricht en voor alle ICT-apparaten waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij Achterhoek VO, ook voor uitzendkrachten en tijdelijke medewerkers.

2.1 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;
- de bescherming van privacygevoelige informatie waaronder persoonsgegevens van Achterhoek VO-medewerkers en -leerlingen (en hun ouders) en daarmee het beschermen van de privacy en veiligheid van alle betrokkenen;
- de bescherming van vertrouwelijke informatie van Achterhoek VO-medewerkers en -leerlingen (en hun ouders);
- het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen;
- de bescherming van de intellectuele eigendomsrechten van Achterhoek VO 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. Achterhoek VO zal dan ook de controle en handhaving van deze regels volgen, en deze in overeenstemming met 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 en daarbij de inzage in deze informatie tot het noodzakelijke minimum beperken. Indien Achterhoek VO geautomatiseerde controle

wenselijk acht vindt voorafgaand een DPIA plaats om tot een zorgvuldige belangenafweging te komen en daarbij de privacy van betrokken optimaal te waarborgen. Zie ook hoofdstuk 4.

2.2 Eigen verantwoordelijkheid en privégebruik

Het gebruik van door Achterhoek VO verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle ICT-apparaten die voor (school)werk worden gebruikt, worden niet uitgeleend of aan anderen ter beschikking gesteld. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen.

2.3 Verschillende soorten gegevens

Achterhoek VO is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy (IBP) is het beschermen van gegevens. Achterhoek VO 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 Achterhoek VO bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- Vertrouwelijke gegevens; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen Achterhoek VO 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 onder andere aan naamgegevens, emailadressen 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 Achterhoek VO schriftelijk afspraken maakt met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk).

Achterhoek VO heeft een Functionaris Gegevensbescherming (FG) aangesteld. Deze ziet onafhankelijk toe op het naleven van de privacywetgeving. In elk van onze scholen is een IBP-verantwoordelijke aangesteld. Deze medewerker ziet toe op de implementatie van het privacybeleid in de school en is het eerste aanspreekpunt in de school voor alle voorkomende vragen over privacy. 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, dan is er sprake van een beveiligingsincident waaruit mogelijk een datalek kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en Achterhoek VO en moet om die reden dan ook altijd worden gemeld bij de IBP-verantwoordelijke of FG. De FG behandelt een melding vanzelfsprekend vertrouwelijk.

Om op een veilige, verantwoorde en werkbare manier met persoonsgegevens om te gaan maakt Achterhoek VO afspraken over:

- de verwerking en verspreiding van vertrouwelijke gegevens 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 Achterhoek VO goedgekeurde bedrijfsmiddelen;
- bestanden met gevoelige en bijzondere persoonsgegevens die een doel dienen, mogen alleen beveiligd of versleuteld worden uitgewisseld;

- bestanden met gevoelige en bijzondere persoonsgegevens, wanneer deze niet in een leerling- of personeelsadministratie pakket kunnen worden opgeslagen en waarvoor we goed kunnen onderbouwen waarom we die moeten bewaren (geldige AVG grondslag), mogen worden opgeslagen in Teams en op de OneDrive. Na gebruik en als er geen reden meer is om deze bestanden nog langer te bewaren, dienen deze bestanden zo spoedig mogelijk te worden verwijderd.

Van medewerkers van Achterhoek VO 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.

3 Gedragscode

In deze gedragscode voor verantwoord gebruik van bedrijfsmiddelen geeft Achterhoek VO 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.

3.1 Algemene normen

Iedere medewerker voldoet aan de volgende algemene normen voor 'zorgvuldigheid' (niet uitputtend):

- Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht;
- Voorkom dat interne en vertrouwelijke informatie in verkeerde handen terechtkomt;
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen (beveiligingsmaatregelen);
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild;
- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering, bij voorkeur door het formulier in te vullen op intranet onder de knop 'beveiligingsincident' (of anders door het sturen van een e-mail aan datalek@achterhoekvo.nl) en stel je IBP- en ICT-medewerker in je school / locatie hiervan op de hoogte.

3.2 Computergebruik

Voor het uitoefenen van de werkzaamheden stelt Achterhoek VO aan de medewerker computer- en netwerkfaciliteiten (bedrijfsmiddelen) ter beschikking. Het gebruik van deze 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 werkzaamheden;
- Houdt privé en werk gescheiden, sla geen privébestanden op in je persoonlijke OneDrive;
- Omgekeerd geldt ook, sla (persoons)gegevens alleen op de daarvoor aangewezen systemen. (Opslaan van gegevens in public Cloud omgevingen, zoals een persoonlijke Dropbox, Google-drive en andere draagbare mediadragers zoals USB-sticks, is niet toegestaan);
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk;
- Sluit na gebruik de computer af of log uit;
- Meld storingen van beheerde werkplekken (computer of laptop) bij je ICT-medewerkers in jouw school / op jouw locatie.

3.3 Werkplek

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen waartoe zij geen rechten hebben en/of laat gegevens niet (onbedoeld) in verkeerde handen terechtkomen. 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 / laptop (windowstoets+L);
- Verwijder interne en vertrouwelijke documenten van het bureau bij het voor langere tijd verlaten van de werkplek (dit geldt ook na 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-mailprogramma af en zorg voor een opgeruimd digitaal bureaublad;
- Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan;
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar.

LET OP: 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. Weet dat beveiligingsincidenten en mogelijke datalekken **altijd** gemeld moeten worden bij de IBP-verantwoordelijke in jouw school / op jouw locatie.

3.4 Gebruik eigen ICT-apparaten

Beveiligingsmaatregelen hebben betrekking op alle ICT-apparaten waarmee werkzaamheden voor Achterhoek VO worden uitgevoerd. Achterhoek VO is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om haar eigen bedrijfsmiddelen.

Voor eigen ICT-apparaten die medewerkers (ook) gebruiken voor het werk ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

- Beveilig het apparaat met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode die langer is dan 4 tekens of met een vingerafdrukscan/gezichtsherkenning/patroon bij een mobiel/tablet;
- Vergrendel het apparaat bij het verlaten van de werkplek;
- Sla geen persoonsgegevens op het eigen apparaat op, dit is niet toegestaan;
- Sla geen persoonsgegevens op een usb-stick of andere draagbare mediadragers op, dit is niet toegestaan;
- Houd software up-to-date door het regelmatig uitvoeren van periodieke updates;
- Neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het regelmatig scannen van het apparaat.

In toenemende mate is het mogelijk beleidsmaatregelen waarover overeenstemming is bereikt, technisch af te dwingen. Achterhoek VO mag controles uitvoeren of de bovenstaande beveiligingsmaatregelingen zijn toegepast.

3.5 Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal in de scholen is niet meer weg te denken. Dit lesmateriaal staat steeds meer online waarbij 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 op apparaten voor persoonlijk gebruik (laptops) kan alleen via de in Software Center beschikbaar gestelde applicaties. Adobe software kan via Adobe Creative Cloud Applicatie worden geïnstalleerd.
- Binnen teams gelden er een aantal beperkingen voor het toevoegen van apps. De volgende type apps zijn toegestaan:
    - Apps die geen persoonsgegevens verwerken;
    - Apps waarvoor een verwerkersovereenkomst is ondertekend en waarvoor het privacy-convenant is ondertekend.

LET OP: Gegevens uit de apps moeten binnen de Europese Economische Ruimte (EER) blijven en mogen niet voor commerciële doelen worden gebruikt. Het gebruik van onlinesoftware, apps en digitaal lesmateriaal waarbij persoonsgegevens verwerkt worden is alleen toegestaan als er een verwerkersovereenkomst wordt afgesloten. Dit geldt voor elke leverancier van (online)software die persoonsgegevens verwerkt en moet vóór gebruik van de app worden geregeld.

3.6 Gebruik van e-mail

Achterhoek VO 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 gaan uit van de volgende afspraken:

- Gebruik het werk e-mailadres alléén voor werk gerelateerde zaken;
- Gebruik voor privé e-mail een eigen privé e-mailadres via een externe web maildienst. (bijvoorbeeld webmail van Gmail, Hotmail of een eigen provider);
- Ontvangen van privé e-mail op het werk e-mailadres is incidenteel toegestaan;
- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie;
- Het is niet toegestaan om het privé e-mailaccount te gebruiken voor het versturen van werkmail;
- 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 werk e-mail met een eigen apparaat (tablet, telefoon) dan kan Achterhoek VO bij verlies of diefstal van het apparaat, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee onverhoopt alle (privé)gegevens van het apparaat worden gewist.

3.6 Gebruik intranet

Medewerkers die vanuit huis het intranet van Achterhoek VO en scholen raadplegen, moeten hiervoor de standaard inloggegevens gebruiken met daarbij de verplichte twee-staps-verificatie.

Veel van de op intranet geregistreerde informatie is uitsluitend bestemd voor de medewerkers van Achterhoek VO en mag niet aan derden bekend worden gemaakt.

3.7 Gebruik van internet

Achterhoek VO stelt het gebruik van internet op het werk en de bijbehorende faciliteiten aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik hiervan moet dus verbonden zijn 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 wordt gebruikt;
- en geen verboden gebruik oplevert.

Het is niet toegestaan om:

- internetsites 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;
- 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 het werk verbonden personen en activiteiten. Dit geldt ook voor internetgebruik buiten het Achterhoek VO-netwerk met betrekking tot aan het werk verbonden personen en activiteiten.

3.8 Veilig online

We brengen met z'n allen steeds meer tijd online door. Hierbij worden steeds meer mobiele apparaten gebruikt. Menselijk (online)handelen staat veelal aan de basis van een datalek.

Achterhoek VO 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 school en Achterhoek VO;
- controleren of er daadwerkelijk van een bekend (bijvoorbeeld het Achterhoek VO-netwerk, eduroam of het eigen draadloze netwerk thuis) én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes.

3.9 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.

Bij het gebruik van sociale media geldt als uitgangspunt dat het digitale gedrag op sociale media niet afwijkt van het gewenste gedrag binnen de school / op de werkplek. Medewerkers worden gemakkelijk gezien als vertegenwoordiger van een school / Achterhoek VO, ook als zij online een privémening verkondigen. Bij Achterhoek VO gelden de volgende afspraken voor het gebruik van sociale media (zie hiervoor ook de Integriteitscode van Achterhoek VO):

- Medewerkers delen op verantwoorde wijze kennis via sociale media, rekening houdend met de goede naam van de school en Achterhoek VO, en iedereen die hierbij betrokken is. Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn;
- Bij onderwerpen maken medewerkers duidelijk of er op persoonlijke titel of namens Achterhoek VO wordt gepubliceerd;
- Medewerkers publiceren geen vertrouwelijke informatie op sociale media;
- Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren, tenzij duidelijk is aangeven dat er namens Achterhoek VO wordt gesproken. Wel is het goed te realiseren dat uitingen die in privé-verband online zijn gedaan ook consequenties kunnen hebben voor de geloofwaardigheid en houdbaarheid van de positie binnen de school / Achterhoek VO;
- Bij twijfel over een publicatie of over de raakvlakken met (het beleid van) Achterhoek VO zoeken medewerkers vóór publicatie contact met een leidinggevende;
- Medewerkers gebruiken voor de communicatie met leerlingen geen WhatsApp, maar alleen door de school / Achterhoek VO gefaciliteerde communicatiemiddelen zoals werk e-mail, chat binnen klassen-Teams en de communicatiemiddelen die binnen een ELO beschikbaar zijn;
- Medewerkers communiceren niet en gaan niet in discussie met een leerling of ouder op sociale media;
- Het is medewerkers niet toegestaan om met een privé account ‘vrienden’ te worden met leerlingen en ouders op sociale media, familie en vrienden kunnen hierop een uitzondering zijn;
- Inzetten van sociale media in het lesprogramma is gebonden aan de toestemming van ouders als leerlingen jonger zijn dan 16 jaar.

3.10 Gebruik beeld- en geluidsmateriaal

Beeld- en geluidsmateriaal van leerlingen (bijvoorbeeld foto’s en video’s met leerlingen herkenbaar in beeld en geluidsfragmenten van leerlingen) wordt niet via e-mail, sociale media of anderszins gepubliceerd of gecommuniceerd zonder de voorafgaande, uitdrukkelijke en aantoonbare

toestemming van de leerling (indien hij 16 jaar of ouder is) dan wel de ouders (als de leerling jonger is dan 16 jaar).

3.11 Wachtwoorden en pincodes

Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en apparaten (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 drie elementen: kleine letter, hoofdletter, cijfer of speciaal teken (!@#$%^&*();
- Iedere medewerker wordt verplicht om gebruik te maken van de twee-staps-verificatie;
- Pincodes (op telefoon of tablet) moeten minimaal uit 4 tekens bestaan of er wordt gebruik gemaakt van een vingerafdruk, gezichtsherkenning en/of patroonbeveiliging;
- Wachtwoorden hoeven niet op gezette tijden te worden gewijzigd omdat er altijd om een twee-staps-verificatie wordt gevraagd. Heb je het vermoeden dat het wachtwoord is gelekt, wijzig deze dan preventief;
- Gebruik niet voor iedere onlinedienst waarbij er een account moet worden aangemaakt, dezelfde gebruikersnaam en/of hetzelfde wachtwoord. Gebruik hiervoor nooit je gebruikersnaam en wachtwoord van het school- / Achterhoek VO-netwerk;
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.

3.12 Meldplicht Datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens de procedure meldplicht datalekken van Achterhoek VO. Meldt deze bij voorkeur door direct een formulier in te vullen voor het melden van een vermeend datalek.
Ze kunnen ook worden gestuurd aan datalek@achterhoekvo.nl. Is het nodig dat de melding strik vertrouwelijk behandeld wordt, stuur dan een e-mail naar fg@achterhoekvo.nl.

4 Controle gebruik bedrijfsmiddelen

Achterhoek VO handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:

- Grondwet;
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018);
- Wet Medezeggenschap Onderwijs (WMO);
- Burgerlijk Wetboek (BW);
- Wetboek van Strafrecht;
- CAO VO.

Achterhoek VO zal bij controle van 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.

4.1 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.
- Als een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode, enkel en alleen in opdracht van de schoolleiding/directie en in afstemming met het bestuur, een gerichte controle plaatsvinden.
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt na akkoord van de schoolleiding/directie en in afstemming met het bestuur controle op de inhoud plaats.
- Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
- Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken medewerker besproken. De schoolleiding/directie 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 GMR onderling, van vertrouwenspersonen, bedrijfsartsen en van eenieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Ook hier kan bij zwaarwegende redenen van worden afgeweken, bijvoorbeeld als de berichten een potentieel gevaar vormen voor onze systemen. Om de veiligheid van onze systemen te waarborgen maken we gebruik van beveiligingssoftware Defender. Het Defender controleproces is belegd bij maximaal twee ICT-medewerkers van het Bestuursbureau. Hiervoor hebben zij separaat een geheimhoudingsverklaring getekend. Dit proces is beschreven in de memo implementatie Beveiligingssoftware Defender die in december 2021 door de GMR is goedgekeurd. In hoofdstuk 4.2 is de werkwijze van deze controle beschreven.

4.2 Uitvoering van de controle

Achterhoek VO beschermt gegevens van leerlingen, medewerkers en ouders tegen misbruik door cybercriminelen (en de hieruit voortvloeiende negatieve publiciteit). Daarom vindt er op alle gebruikte ICT-systemen en internetgebruik een geautomatiseerde controle plaats. Door gebruik te maken van beveiligingssoftware worden alle door de school / Achterhoek VO gefaciliteerde ICT-apparaten en -systemen gescand op mogelijke gevaren. Hiervoor wordt meta-data verzameld en geanalyseerd. Hierdoor krijgen de twee speciaal hiervoor geautoriseerde ICT-medewerkers van Achterhoek VO direct een signalering van mogelijke risico's van buitenaf in beeld. Door een volledig geautomatiseerd proces worden e-mail, bijlages en internetgebruik binnen de scholen softwarematig gescand op

gevaarlijke inhoud. Zo nodig worden ze direct verwijderd. Achterhoek VO beperkt de verwerking van persoonsgegevens bij deze controles door:

- informatie te beperken tot meta-data van verkeers- en opslaggegevens in het kader van kosten- en capaciteitsbeheersing;
- beperkt te controleren, zoals op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is;
- ICT-medewerkers een geheimhoudingsverklaring te laten ondertekenen die 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;
- de nodige maatregelen te treffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn;
- passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

4.3 Disciplinaire maatregelen

Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het bestuur van Achterhoek VO, 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 arbeidsovereenkomst.

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.

4.4 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 meestal geregeld in de arbeidsovereenkomst, regels rondom personeelszaken en/of de van toepassing zijnde CAO.

5 Slotbepaling

De organisatie kan deze gedragscode met instemming van de GMR wijzigen als de omstandigheden daar aanleiding toe geven. Deze regeling wordt minimaal eenmaal in de vijf jaar geëvalueerd door het bestuur van Achterhoek VO en de GMR. Wijzigingen worden voorafgaand aan de invoering ervan aan de medewerkers bekend gemaakt.

In de gevallen waarin de code niet voorziet, waarbij de toepassing niet eenduidig is of tot kennelijke onbillijkheden leidt, besluit het bestuur van Achterhoek VO.