



Gedragscode voor ict- en internetgebruik voor medewerkers

Inhoud

1. Inleiding	2
1.1. Uitgangspunten gedragscode ict- en internetgebruik	2
1.2. Eigen verantwoordelijkheid en privegebruik	3
1.3. verschillende soorten gegevens	3
2. Gedragscode	4
2.1. Algemene normen	4
2.2. Computergebruik	5
2.3. Werkplek	5
2.4. Gebruik eigen devices	6
2.5. Software en digitaal lesmateriaal	6
2.6. Gebruik van e-mail	7
2.7. Gebruik van internet	7
2.8. Veilig online	8
2.9. Sociale media	8
2.10. Gebruik beeld- en geluidsmateriaal	9
2.11. Wachtwoorden en pincodes	9
2.12. Meldplicht beveiligingsincidenten en datalekken	10
3. Controle gebruik bedrijfsmiddelen	10
3.1. Voorwaarden voor controle	10
3.2. Uitvoering van de controle	11
3.3. Disciplinaire maatregelen	11
3.4. Bezwaar en beroep	12

1. Inleiding

Dit document is een specifieke aanvulling op de gedrags- en integriteitscode van Skobos medewerkers. We kiezen voor een apart document, omdat ICT- en internetgebruik nadrukkelijk onder de aandacht moet worden gebracht en onderdeel is van het normenkader IBP.

Beide documenten brengen we bij elke (nieuwe) medewerker onder de aandacht:

- we bespreken ze tijdens de introductie van nieuwe medewerkers;
- we bespreken de gedragscode ICT- en internetgebruik tijdens de AVG-training;
- we maken een verwijzing in het document 'welkom bij Skobos';
- we maken een verwijzing in het document gebruikersovereenkomst;
- de gedragscode ICT- en internetgebruik keert jaarlijks terug in de personeelsnieuwsbrief.

Het gebruik van internet, computernetwerk en e-mail is voor alle medewerkers van Skobos 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 Office 365-omgeving met alle bijbehorende apps, 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 en maar ook sociale media zoals Facebook, LinkedIn, Instagram en X.

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers van Skobos 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 Skobos, ook voor stagiairs, leden raad van toezicht, uitzendkrachten en tijdelijke werknemers.

1.1. Uitgangspunten gedragscode ict- en internetgebruik

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, zijn 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, zijn medewerkers, leerlingen en hun ouders en andere betrokkenen;
- 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. Skobos 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. Het bestuur zal mensen met toegang daartoe contractueel verplichten tot afdoende geheimhouding.

1.2. Eigen verantwoordelijkheid en privegebruik

Het gebruik van door Skobos 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. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen.

1.3. verschillende soorten gegevens

Skobos is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens. SKOBOS 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 Skobos bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- Vertrouwelijke gegevens; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen Skobos 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 Skobos schriftelijk afspraken maakt met

leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk). Skobos heeft een Functionaris voor gegevensbescherming 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 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 Skobos.

Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt Skobos afspraken over:

- de verwerking en verspreiding van vertrouwelijke- 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 Skobos goedgekeurde bedrijfsmiddelen.

Van medewerkers van Skobos en/of externe medewerkers, die vanwege hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bv. personeelsdossiers, leerlingdossiers, 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 Skobos 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, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht.
- Voorkom het lekken van interne en vertrouwelijke informatie.
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen. Laat bedrijfsmiddelen nooit onbeheerd achter (bijvoorbeeld in de auto) en beveilig bedrijfsmiddelen altijd met een wachtwoord.
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild (bijvoorbeeld door jailbreaks).

- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering bij je leidinggevende en stuur een e-mail aan privacy@skobos.nl of een telefonische melding bij de daarvoor aangewezen persoon (Zie hiervoor het protocol beveiligingsincidenten en datalekken van Skobos).
- Wanneer een eigen device wordt gebruikt (zoals een smartphone) voor zakelijke doeleinden, meld verlies of diefstal dan zo snel mogelijk bij jouw leidinggevende en stuur een e-mail aan privacy@skobos.nl of een telefonische melding bij de daarvoor aangewezen persoon (Zie hiervoor het protocol beveiligingsincidenten en datalekken van Skobos). Geef duidelijk aan welke accounts gekoppeld zijn aan het eigen device.

2.2. Computergebruik

Voor het uitoefenen van de werkzaamheden stelt Skobos 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).
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Sluit na gebruik de computer af of log uit.
- Laat geen andere personen werken op jouw account.
- Schoon regelmatig (minimaal 4x per jaar) je mailbox op (ook verzonden items) en je OneDrive (maximaal 15GB).
- Meld storingen van beheerde werkplekken (computer of laptop) bij de ict-afdeling via admskobos@skobos.nl.

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 mee kan kijken. Zorg ervoor dat je instellingen voor de weergave van meldingen in Teams juist zijn, sluit het e-mail programma af en laat geen documenten op je digitale bureaublad staan.
- Laat geen afdrucken bij de printer liggen, zeker niet als er persoonsgegevens op staan. Skobos-medewerkers maken allen gebruik van beveiligd printen door middel van gebruik van een printerpas/printcode.
- 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 gemeld moeten worden volgens het protocol beveiligingsincidenten en datalekken van Skobos.

2.4. Gebruik eigen devices

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor Skobos worden uitgevoerd. Skobos is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school. Skobos stelt deze beveiligde bedrijfsmiddelen/devices beschikbaar voor de werknemer.

Voor 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 of met touch ID of gezichtsherkenning. Zie 2.11 Wachtwoorden en pincodes.
- Vergrendel het device bij het verlaten van de werkplek (windowstoets+L).
- Sla vertrouwelijke informatie en persoonsgegevens van Skobos niet op het eigen device op; dit is niet toegestaan.
- Scheid (versleutelde)gegevens, anders dan persoonsgegevens, van Skobos 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.
- Meld verlies of diefstal van eigen devices die gekoppeld zijn aan een zakelijk account altijd bij jouw leidinggevende en stuur een e-mail aan privacy@skobos.nl of een telefonische melding bij de daarvoor aangewezen persoon (zie hiervoor het protocol beveiligingsincidenten en datalekken van Skobos).

2.5. Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal is niet meer weg te denken bij Skobos. 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 bekiikt 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:

- Gebruik van online software wordt bij Skobos alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen.
- Bij het gebruik van online software, app's 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 Skobos persoonsgegevens verwerkt. Regel dit vooraf aan het gebruik. Getekende verwerkersovereenkomsten zijn voor alle medewerkers te vinden in Teams Medewerkers.
- Voor het beheer van vertrouwelijke gegevens maakt Skobos uitsluitend gebruik van systemen die beveiligd worden met een wachtwoord, bij voorkeur in combinatie met het gebruik van twee-factor-authenticatie (2FA).
- Bij het gebruik van twee-factor-authenticatie maken medewerkers indien mogelijk gebruik van de app Microsoft Authenticator.
- Wanneer systemen de mogelijkheid bieden om via SSO (Single Sign-On) in te loggen, dan doen medewerkers van Skobos dat.
- Volg bij het aanvragen van digitaal lesmateriaal en/of andere software de afgesproken aanvraagprocedure van Skobos. Hiervoor is een aanvraagformulier beschikbaar wat als uitgangspunt dient voor eventuele wettelijk verplichte aanvullende privacy- en/of beveiligingsmaatregelen.

2.6. Gebruik van e-mail

Skobos stelt een e-mailsysteem en een bijbehorende mailbox aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden (Microsoft Outlook). Gebruik van e-mailfaciliteiten is verbonden aan deze werkzaamheden en gaan uit van de volgende afspraken:

- Gebruik het Skobos e-mailadres alléén voor werkgerelateerde zaken. Dit e-mailadres is gekoppeld aan het Office 365-account van de medewerker en dat wordt uitsluitend gebruikt voor werkgerelateerde doeleinden.
- Gebruik voor privé e-mail een eigen privé e-mailadres via een externe webmaildienst. (bijvoorbeeld webmail van Gmail, Hotmail of een eigen provider).
- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.
- Het is niet toegestaan e-mail te gebruiken voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of berichten die kunnen aanzetten tot haat en geweld.
- Synchroniseert een medewerker de werk e-mail met een eigen device (tablet, telefoon) dan kan Skobos, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om het Office 365-account te verwijderen of het betreffende wachtwoord te wijzigen.

2.7. Gebruik van internet

Skobos 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;
 - 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. Skobos 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 SKOBOS;
- controleren of er daadwerkelijk van een bekend én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes. (Een netwerk kan bekend zijn omdat het een SKOBOS-netwerk is, eduroam of het eigen draadloze netwerk thuis is).

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, X, 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/organisatie. Medewerkers moeten zich realiseren dat zij, ook als zij online een privémening verkondigen, altijd kunnen worden gezien als vertegenwoordigers van Skobos.

Bij Skobos gelden de volgende afspraken voor het gebruik van sociale media:

- Onder werktijd gebruik je sociale media uitsluitend voor werkgerelateerde zaken.
- Deel op verantwoorde wijze kennis via sociale media rekening houdend met de goede naam van Skobos en iedereen die hierbij betrokken is.

- Maak bij onderwijsgerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens Skobos/de school gedaan wordt.
- Bestuurders, directeuren en leidinggevenden zijn altijd vertegenwoordiger van Skobos en/of het kindcentrum – ook als zij een privémening verkondigen. Bij twijfel niet publiceren.
- Publiceer geen vertrouwelijke informatie op sociale media.
- Publiceer geen beeldmateriaal van leerlingen zonder de uitdrukkelijke voorafgaande aantoonbare toestemming van ouders als de leerling jonger is dan 16 jaar of van de leerling zelf als deze 16 jaar of ouder is.
- Publiceer geen beeldmateriaal van leerlingen in badkleding en/of ontbloot bovenlijf.
- Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn. Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren.
- Neem contact op met een leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met Skobos/de school.
- Het is medewerkers niet toegestaan om met een privéaccount 'vrienden' te worden met leerlingen op sociale media.
- Ga niet in discussie met een leerling of ouder op sociale media.
- Houd rekening met het wettelijk vastgelegde auteurs-, beeld- en citaatrecht. Het is verboden om zonder toestemming van de maker andermans werk te publiceren. Schending van deze wet kan je een boete opleveren van honderden euro's.
- Inzetten van sociale media in het lesprogramma is gebonden aan de toestemming van ouders als leerlingen jonger zijn dan 16 jaar.

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 Skobos mag alleen als daar vooraf toestemming voor gegeven is door ouders/verzorgers als de leerling jonger is dan 16 jaar of de leerling zelf als deze 16 jaar of ouder is. Zonder deze toestemming mogen geen foto's, video's en geluidsfragmenten van leerlingen gebruikt worden.

- Skobos verwijst hierbij naar de richtlijn die is opgesteld 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.
- Foto's, video's en geluidsfragmenten van medewerkers mogen alleen gebruikt worden wanneer de betreffende medewerker hiervoor mondelinge en/of schriftelijke toestemming heeft gegeven.

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 en zijn een combinatie van de volgende elementen: kleine letter, hoofdletter, cijfer en speciaal teken (!@#\$%^&*()).

- Pincodes (op telefoon of tablet) moeten langer zijn dan 4 tekens, tenzij er maar 4 tekens mogelijk zijn.
- Bij uitgifte van een Office 365-account ontvangt een nieuwe medewerker een door Skobos aangeleverd tijdelijk wachtwoord. Wanneer de medewerker hiermee inlogt in Office 365, dient direct een persoonlijk wachtwoord te worden ingesteld.
- Medewerkers van Skobos veranderen minimaal één keer per jaar alle wachtwoorden die ze voor hun werk gebruiken, aan het begin van het schooljaar. Hierbij kiezen ze een volledig nieuw wachtwoord, dat nog niet eerder is gebruikt. Aanpassing van enkele tekens is niet voldoende.
- Gebruik niet voor elke systeem hetzelfde wachtwoord.
- Zorg ervoor dat anderen jouw wachtwoorden en inloggegevens niet kunnen vinden of achterhalen. Medewerkers die hun wachtwoorden en inloggegevens ergens willen bewaren, doen dit niet op papier, maar in een digitale, afgeschermd omgeving zoals hun OneDrive.
- Deel wachtwoorden en inloggegevens nooit, ook niet incidenteel. Wachtwoorden en inloggegevens zijn persoonlijk.

2.12. Meldplicht beveiligingsincidenten en datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens het protocol beveiligingsincidenten en datalekken van Skobos.

3. Controle gebruik bedrijfsmiddelen

Bij Skobos is elkaar vertrouwen uitgangspunt. Skobos handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:

- De Grondwet;
- Algemene Verordening Gegevensbescherming (AVG);
- Wet Medezeggenschap Onderwijs (WMO);
- Burgerlijk Wetboek (BW);
- Wetboek van Strafrecht;
- Cao po.

Skobos 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 Skobos gerichte controle plaatsvinden.

- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van SKOBOS, 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. SKOBOS 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 een ieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Dit geldt niet voor veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.

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 contentfiltering.
- De controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze contentfiltering. Verdachte berichten worden apart gezet voor nader onderzoek.
- De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens.
- 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 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 SKOBOS worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- Door SKOBOS 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

Gedrag in strijd met deze gedragscode of bij sterke vermoedens van dergelijk gedrag hoort direct bij de leidinggevende gemeld te worden. Op overtredingen van de regels kunnen, afhankelijk van het feitencomplex, de ernst van de overtreding, hetgeen in de cao-po, het Burgerlijk Wetboek, wet- en regelgeving, statuten reglementen en jurisprudentie, na afweging door het CvB verschillende maatregelen genomen worden. Maatregelen kunnen variëren van een waarschuwing tot ontslag op staande voet. Daargelaten een eventuele eis tot schadevergoeding of aangifte bij justitiële autoriteiten.

We maken voor de helderheid een globaal onderscheid in drie fasen;

Fase 1 (Geel):

Een waarschuwing kan aan de orde zijn bij onbewust en onbedoeld gedrag. Herstel is mogelijk en ongewenst gedrag kan worden omgebogen naar gewenst gedrag.

Fase 2 (Oranje):

Er kan ook een laatste waarschuwing of afhankelijk van de ernst van de gedraging een disciplinaire maatregel (zoals een schorsing of een berisping) gegeven worden wanneer ongewenst gedrag van fase 1 meerdere malen voorkomt. Dit is de oranje fase. Hiertoe kan het CvB na afweging van de feiten en omstandigheden en hetgeen in de cao-po, het Burgerlijk Wetboek, wet- en regelgeving, statuten reglementen en jurisprudentie is vermeld, overgaan. Een volgende overtreding kan dan fase 3 zijn.

Fase 3 (Rood):

Bij deze fase kan een beëindiging van de arbeidsovereenkomst (eventueel door het starten van een gerechtelijke procedure) aan de orde zijn. Hiertoe kan het CvB na afweging van de feiten en omstandigheden en hetgeen in de cao-po, het Burgerlijk Wetboek, wet- en regelgeving, statuten reglementen en jurisprudentie is vermeld, overgaan. Het is mogelijk dat eerst al een maatregel in fase oranje of geel is afgegeven, maar afhankelijk van de ernst van de gedraging kan ook direct overgegaan worden naar fase rood.

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. Bezwaar kan de medewerker maken bij CvB en beroep via cao po artikel 12.1.