Gedragscode ICT

Omgaan met bedrijfsmiddelen

Inhoud

1 Inleiding en uitgangspunten gedragscode ICT

1.1 Inleiding

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. We vragen van onze medewerkers en leerlingen om verantwoord om te gaan met de beschikbare middelen. Onze code is bedoeld voor iedereen die werkzaam is binnen onze stichting, ook voor uitzendkrachten, tijdelijke werknemers (gedetacheerden) en stagiaires. De code is er ook voor alle externen die, via een account van onze stichting, toegang hebben tot de bedrijfsmiddelen van de organisatie. Het gebruik van door stichting middelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker.

1.2 Waarom een ICT-gedragscode

De code is er opgericht om het gebruik van ICT binnen onze stichting veilig, snel en betrouwbaar te houden. We streven met deze code verschillende doelen na:

- Systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik.
- Tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten.
- De bescherming van privacygevoelige informatie waaronder persoonsgegevens van de medewerkers, stagiaires, leerlingen en ouders en daarmee het beschermen van de privacy en veiligheid van alle betrokkenen.
- Bescherming van vertrouwelijke informatie van Stichting Optimus Primair Onderwijs en van medewerkers, stagiaires, leerlingen en ouders.
- Het voorkomen en tegengaan van misbruik van bedrijfsmiddelen.
- De bescherming van de intellectuele eigendomsrechten van Stichting Optimus Primair Onderwijs en derden.
- Het voorkomen van negatieve publiciteit.
- Kosten- en capaciteitsbeheersing.

1.3 Onze algemene normen

We vragen van je:

- 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 door het sturen van een e-mail aan privacycoordinator@optimusonderwijs.nl of een telefonische melding naar de Privacy Officer (06-34854011), (Zie hiervoor ook de procedure meldplicht datalekken van Stichting Optimus Primair Onderwijs).
- 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.

Bij twijfel, neem contact op met de Privacy en Security Officer van de stichting.

2 Dit zijn onze afspraken

2.1 Computergebruik

We vragen van je:

- Sla (persoons)gegevens alleen op in de daarvoor aangewezen systemen.
- Deel bestanden zo veel als mogelijk via een link en niet als bijlage.
- Installeer software die wordt aangeboden vanuit de stichting.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Gebruik niet voor elk systeem hetzelfde wachtwoord.
- Maak waar mogelijk gebruik van een extra identiteiten controle (MFA / 2- wegverificatie).
- Gebruik geen extern opslagmedium (USB- sticks, externe harde schijf, usbflasdrives)
- Sluit na gebruik de computer af of log uit.
- Meld storingen van beheerde werkplekken bij de ICT-helpdesk (helpdesk@ipos-ict.nl)
- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.
- Weet welke ICT-voorzieningen je mag gebruiken.
- Versleutel alle gegevens met betrekking van de stichting, indien deze gegevens, om welke reden dan ook, elders opgeslagen worden.

2.2 Gebruik van e-mail

We vragen van je:

- Gebruik het school e-mailadres alléén voor je werk.
- Gebruik voor privé e-mail en privé zaken een eigen privé e-mailadres.
- Ontvangen van privé e-mail op het zakelijke e-mailadres is niet 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.

2.3 Werkplek

We vragen van je:

- Vergrendel bij het verlaten van de werkplek de computer (Windowstoets + L).
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm mee kan kijken.
- Sluit het e-mail programma af en zorg voor een opgeruimd digitaal bureaublad.
- Print met code en laat geen afdrukken bij de printer liggen.
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar.

2.4 Gebruik eigen middelen (BYOD)

We vragen van je:

- Beveilig het device met een verificatie methode (wachtwoord, of in het geval van een smartphone of tablet, met een pincode of veegpatroon)
- Vergrendel het device bij het verlaten van de werkplek (Windowstoets + L of lockscreen).

- Sla persoonsgegevens van de stichting niet op het eigen device op of op een externe opslag-mediums zoals een usbstick
- Sla persoonsgegevens van de stichting niet op buiten de applicaties die hiervoor binnen de organisatie bedoeld zijn, zoals de systemen en apps van Office 365, ParnasSys.
- Scheid (versleutelde) gegevens van de stichting en privégegevens van elkaar.
- 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.

Bij gebruik van een eigen middel ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij jezelf.

2.5 Wachtwoorden en pincodes

We vragen van je:

- Gebruik een minimaal 8 tekenwachtwoord, met minstens twee van de volgende vier elementen: kleine letter, hoofdletter, cijfer of speciaal teken (!@#$%^&*()
- Verander met regelmaat je wachtwoord.
- Beveilig de toegang tot devices met een pincode of veegpatroon.
- Gebruik niet voor elk systeem hetzelfde wachtwoord, indien geen MFA/2- wegverificatie wordt gebruikt.
- Gebruik bij systemen die veel persoonsgevoelige informatie bevatten (zoals ParnasSys en O365) altijd een MFA/2-wegverificatie
- Deel wachtwoorden nooit, ook niet incidenteel.

2.6 Software en digitaal lesmateriaal

- Binnen onze stichting installeren we alleen bedrijfssoftware met de juiste licenties en indien nodig na het nemen van aanvullende maatregelen. Een licentie kan alleen in samenhang met een door het C.v.B getekende verwerkersovereenkomst worden afgesloten.

2.7 Intellectueel eigendom en vertrouwelijke informatie

We vragen van je:

- Om vertrouwelijke en/of privacygevoelige informatie strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.
- Maak geen inbreuk op de intellectuele eigendomsrechten van stichting en derden en respecteert licentieafspraken die van toepassing zijn binnen de organisatie.

2.8 Gebruik van internet

We vragen van je:

- Beperkt persoonlijk gebruik is toegestaan zolang dit niet storend is, 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
- auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron
- deel te nemen aan kansspelen.
- Met dreigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren.

2.9 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.

We vragen van je:

- het onderscheid te herkennen tussen betrouwbare en onbetrouwbare websites.
- alleen bekende én beveiligde draadloze netwerken te gebruiken.
- een phishingsmail en malware te herkennen en dat je weet hoe je moet handelen.

2.10 Sociale media

Je mag kennis en informatie over de school en/of stichting delen op sociale media mits het geen persoonsgegevens[1] en/of vertrouwelijke informatie is die de school of andere betrokkenen schaadt.

We vragen van je:

- Dat je de reguliere fatsoensnormen in acht neemt. Gedragingen en uitlatingen, zoals pesten, kwetsen, stalken, bedreigen, hacken, radicalisering en sexting zijn uit den boze.
- Om geen beeld- en/of geluidsopnamen te maken en/of te verspreiden, tenzij door de schooldirecteur hiervoor nadrukkelijk vooraf expliciet toestemming is gegeven.
- Maak voor communicatie over werk gerelateerde onderwerpen gebruik van de formele kanalen van de stichting (zoals Teams, WooW, Sharepoint en het zakelijke (@optimusonderwijs.nl) mailaccount e.d.)
- Weet dat gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zijn, ook na verwijdering van het bericht.
- Om ontoelaatbare en/of grensoverschrijdende communicatie in woord, beeld en/of geluid te melden bij de schooldirecteur, leidinggevende of het College van Bestuur.
- Handel bewust, je bent altijd zelf verantwoordelijk voor de inhoud die je publiceert, doorstuurt of herplaatst op Social Media.

[1] Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, e-mailadres, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4 AVG).

2.11 Gebruik beeld- en geluidsmateriaal

Je mag alleen beeld- en geluidsmateriaal van medewerkers, stagiaires en leerlingen delen als hier vooraf schriftelijk toestemming voor is gegeven.

2.12 Meldplicht Datalekken

Ontdek je een beveiligingsincident en mogelijk datalek dan verwachten we dat je hier melding van maakt. Stuur een bericht naar privacycoordinator@optimusonderwijs.nl of bel naar 06- 51733747

Onze protocol Melden datalek kun je hier vinden.

3 Controle, Voorwaarden, uitvoering controle

3.1 Controle gebruik bedrijfsmiddelen

Bij de controle op het gebruik van bedrijfsmiddelen handelen we binnen de geldende wet- en regelgeving. Als basis gaan we uit van deze gedragscode.

3.2 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.
- Uitsluitend bij een ernstig vermoeden van schending van deze gedragscode door een medewerker of een groep medewerkers, kan gedurende een vastgestelde (korte) periode, in opdracht van het College van Bestuur gerichte controle op individueel gebruik van bedrijfsmiddelen plaatsvinden.
- Gerichte controle en onderzoek vinden uitsluitend plaats na schriftelijke opdracht van het College van Bestuur, na advies van Juridische Zaken, waarbij de reden vermeld zal worden waarom tot dit gerichte onderzoek zal worden overgegaan. Het onderzoek wordt uitgevoerd door één of meer daartoe aangewezen medewerker(s) van de technische ict- dienst.
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van het College van Bestuur, controle op de inhoud plaats.
- Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken medewerker besproken. We zullen 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 medezeggenschap, van vertrouwenspersonen, bedrijfsartsen en van eenieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Dit geldt niet voor de (technische) veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden, indien het berichtenverkeer niet veilig gebeurt.

3.3 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. Verdachte berichten worden apart gezet voor nader onderzoek.
- 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 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 de stichting worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.

- Door stichting worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

4 Bijlage: verwijzingen

- Protocol datalekken: Klik hier om te downloaden.
- Gedragscode webpagina medewerkers: Klik hier om de pagina te openen.