Gedragscode voor ICT- en internetgebruik voor medewerkers van Scholenstichting De Stroming

Datum: oktober 2024

	Directieberaad	College van Bestuur	Raad van Toezicht	Gemeenschappelijke Medezeggenschapsraad
Vergaderdatum	12 november 2024	12 november 2024	januari 2025	januari 2025
Besluitvorming	*Advies*	*Vaststellen*	*Goedkeuren*	*Instemming*

Acceptable Use Policy
Dit document dient als gedragscode voor ICT- en internetgebruik van werknemers van De Stroming, verder te noemen de Gedragscode.

Basis voor de gedragscode
Het gebruik van internet en ICT-middelen is voor (veel van) de werknemers binnen de instelling noodzakelijk om hun werk goed te kunnen doen. Aan het gebruik hiervan zijn echter risico's verbonden die nopen tot het stellen van gedragsregels. Tegen de achtergrond van deze risico's mag van de werknemers verantwoord gebruik van internet en ICT worden verwacht.

Met deze Gedragscode wil De Stroming regels stellen omtrent het gewenst gebruik van deze bedrijfsmiddelen. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT- en internetgebruik en de privacy van de werknemer.
Het gebruik van sociale media wordt steeds belangrijker maar kan ook zijn weerslag hebben op De Stroming. Daarom willen we ook hier bepaalde regels aan verbinden.
De Stroming is als werkgever bevoegd om regels te stellen omtrent de uitvoering van het werk en de goede orde op de werkvloer. De Gedragscode is ook gebaseerd op de wet.
Omdat de Gedragscode voorziet in een verwerking van persoonsgegevens en/of controle op gedrag of prestaties van werknemers, is de Gemeenschappelijke Medezeggenschapsraad (GMR) instemmingsplichtig.

1. Uitgangspunten

1.1. De Gedragscode stelt regels ten aanzien van het gebruik van de bedrijfsmiddelen ICT en internet door werknemers. Doel van deze regels is de goede orde te bepalen ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
- tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
- bescherming van privacy gevoelige informatie waaronder persoonsgegevens van de werknemers en van leerlingen en ouders;
- bescherming van vertrouwelijke informatie van De Stroming en haar werknemers, en van leerlingen en ouders;
- bescherming van de intellectuele eigendomsrechten van De Stroming en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen De Stroming;
- voorkomen van negatieve publiciteit;
- bescherming van bedrijfsmiddelen tegen misbruik.

1.2. Beperkt privégebruik van internet en ICT-middelen is alleen toegestaan voor zover het werk er niet onder lijdt.

1.3. De Gedragscode geldt voor een ieder die voor De Stroming werkzaam is, dus ook voor uitzendkrachten en tijdelijke werknemers. Voor gasten van werknemers geldt de Gedragscode eveneens.

1.4. De Stroming streeft in het kader van handhaving van de Gedragscode naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele werknemers zo veel mogelijk beperken.

2. Intellectueel eigendom en vertrouwelijke informatie

2.1. De werknemer dient vertrouwelijke informatie, privacygevoelige informatie waaronder persoonsgegevens waar hij in het kader van het werk toegang tot heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.

2.2. De werknemer mag geen inbreuk maken op de intellectuele eigendomsrechten van De Stroming en derden en respecteert de licentie-afspraken zoals die van toepassing zijn binnen de Instelling.

2.3. De zeggenschap over de informatie van De Stroming berust bij De Stroming. De werknemer heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door De Stroming.

3. Gebruik van computer- en netwerkfaciliteiten

3.1. Computer- en netwerkfaciliteiten worden aan de werknemer voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in 1.2.

3.2. De werknemer dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen. Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik van een wachtwoord kan het systeembeheer per direct het betrokken account ontoegankelijk maken.

3.3. De Stroming kan voor onderwijs- en andere bedrijfsdoeleinden systemen of applicaties voorschrijven, zoals een Elektronische LeerOmgeving, een e-mailsysteem, (Mobiele) applicaties (Apps), Cloudvoorzieningen of multimediadiensten. De werknemer zal voor het delen van lesmateriaal of het uitvoeren van onderzoek alleen deze systemen gebruiken en de daarbij gestelde beperkingen en eisen stipt naleven.

4. Gebruik van e-mail en andere ICT-communicatiemiddelen (op zakelijke en op prive-apparaten)

4.1. Het e-mailsysteem en de bijbehorende mailbox en e-mailadres wordt aan de werknemer voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

4.2. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in 1.2.

4.3. Gebruik, privé of ten behoeve van studie, mag niet storend zijn voor de goede orde bij De Stroming en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van De Stroming of derden of de integriteit en de veiligheid van het netwerk aantasten. Onder storend en/of overlast veroorzakend gebruik wordt in ieder geval verstaan

- het verzenden van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud;
- het verzenden van berichten met een (seksueel) intimiderende inhoud;
- het verzenden van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
- het versturen van ongevraagde berichten aan grote aantallen ontvangers, kettingbrieven te versturen of kwaadaardige software zoals virussen, Trojaanse paarden of spyware te versturen.

4.4. De werknemer gebruikt voor privé-mail bij voorkeur niet het door De Stroming verstrekte e-mailadres, binnen de grenzen van 1.2. De organisatie zal de toegang tot andere e-maildiensten niet blokkeren of specifiek monitoren.

4.5. In geval van ziekte, onverwacht langdurige afwezigheid of grove nalatigheid van de werknemer, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert, is De Stroming gerechtigd een vervanger of leidinggevende toegang tot de bestanden of mailbox van de werknemer te verschaffen doch uitsluitend indien aangetoond kan worden dat toestemming van de werknemer verkrijgen onmogelijk is of het bedrijfsbelang zodanig zwaar is dat toestemming niet vereist hoeft te worden.
Deze mag zich echter geen toegang verschaffen tot als privé gemarkeerde mappen, als privé herkenbare mails, of mails verzonden naar dan wel afkomstig van een vertrouwenspersoon / bedrijfsarts / HR-consulent. Indien de werknemer geen dergelijke markeringen heeft aangebracht, kan De Stroming door inschakeling van een vertrouwenspersoon de betreffende informatie van de werknemer controleren om zo privé informatie te herkennen en apart te plaatsen alvorens de vervanger of leidinggevende toegang krijgt.

4.6. De inhoud van E-mailberichten wordt niet gecontroleerd. Dit geldt niet voor geautomatiseerde controle (logging en monitoring) op de veiligheid van het e-mailverkeer en netwerk.

Gebruik van zakelijke e-mails/informatie of apps op privé-apparaten.

4.7 Toestemming en Verantwoording:
Werknemers mogen zakelijke e-mail alleen op privé-apparaten ontvangen wanneer hiervoor toestemming is gegeven door de IT-afdeling of leidinggevende.

4.8 Beveiliging van het Apparaten:

- Zorg ervoor dat het apparaat is beveiligd met een sterke toegangscode, wachtwoord, vingerafdruk of gezichtsherkenning.
- Activeer de schermvergrendeling na maximaal 5 minuten inactiviteit.
- De e-mailaccount moet kunnen worden verwijderd op afstand (door IT-beheer) in geval van verlies of diefstal van het apparaat.

4.9 Gebruik van Beveiligde Software:
Gebruik uitsluitend de goedgekeurde applicatie voor toegang tot zakelijke e-mails en instellingen. Het gebruik van niet-goedgekeurde software kan leiden tot beveiligingsrisico's en is daarom niet toegestaan.

4.10 Beveiligingsupdates en Antivirussoftware:
Het privé-apparaat moet regelmatig worden geüpdatet en voorzien zijn van antivirussoftware, om de beveiliging tegen malware te waarborgen.

4.11 Geen Delen van Zakelijke Gegevens:
Zakelijke e-mails en informatie die op privé-apparaten staan, mogen niet worden gedeeld met anderen, inclusief familieleden of vrienden.

4.12 Vermijden van Openbare Netwerken: Vermijd het ophalen van zakelijke e-mail via onbeveiligde, openbare wifi-netwerken. Maak bij voorkeur gebruik van een VPN-verbinding bij gebruik van een openbaar netwerk.

4.13 Melden van Incidenten:

Bij verlies, diefstal of verdenking van een datalek is de werknemer verplicht dit direct te melden aan de IT-afdeling. Hiermee kunnen gepaste maatregelen worden genomen.

4.14 Verwijderen van Zakelijke Gegevens bij Beëindiging van Dienstverband:
Bij vertrek uit het bedrijf dient de werknemer alle zakelijke gegevens van het privé-apparaat te verwijderen en het account te laten deactiveren door de IT-afdeling.

5. Gebruik van internet

5.1. De toegang tot internet en bijbehorende faciliteiten worden aan de werknemer voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

5.2. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in 1.2.

5.3. Verboden tijdens werktijd en / of bij het gebruik van Stromings netwerk / Internetverbinding is echter:

- ongewenst gedrag;
- filesharing- of streamingdiensten te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de faciliteiten in gevaar kan brengen;
- films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de werknemer daadwerkelijk weet dat dit in strijd met auteursrechten is;
- films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

5.4 Er mag alleen beperkt gebruik worden gemaakt van openbare WIFI.

6. Gebruik van sociale media

6.1. Persoonsgegevens of gevoelige gegevens van anderen dienen niet via sociale media gedeeld te worden.

6.2. De Stroming accepteert de open dialoog en de uitwisseling van ideeën en het delen van kennis van de werknemer met vakgenoten en derden via sociale media. Indien dit werk gerelateerde onderwerpen betreft, dient de werknemer ervoor te zorgen dat het profiel en de inhoud in overeenstemming is met hoe hij zich in tekst, beeld en geluid zou presenteren ten overstaan van collega's en leerlingen.

6.3. Bestuurders, managers, leidinggevenden en anderen die namens De Stroming beleid of strategie uitdragen hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media, ook als de inhoud niet direct verband houdt met hun werk. Op grond van hun positie moeten zij nagaan of zij op persoonlijke titel kunnen publiceren. Zij moeten zich ervan bewust zijn dat werknemers lezen wat zij schrijven.

6.4. Dit geldt ook indien werknemers vanaf privécomputers of -internetaansluitingen deelnemen aan sociale media, doch uitsluitend voor zover het gaat om deelname die het werk kan raken.

6.5. Wanneer werknemer een sociale-media-account opzet dat direct werkgerelateerd is, terwijl het op naam van werknemer persoonlijk is gesteld, zullen werknemer en De Stroming bij beëindiging van het dienstverband een passende oplossing zoeken voor het overdragen van dit profiel of de informatie en contacten daarop.

6.6 Beeldmateriaal van 5 jaar en ouder (waarop herkenbare gezichten van leerlingen te zien zijn) wordt aan het einde van elk schooljaar verwijderd van de social media kanalen van de scholen.

6.7 Werknemers mogen via social media niet bevriend zijn met leerlingen.

6.8 Als online communicatie dreigt te ontsporen dient de medewerker direct contact op te nemen met zijn/haar leidinggevende om de te volgen strategie te bespreken.

6.9 Het is voor betrokkenen niet toegestaan om foto-, film- en geluidsopnamen van schoolgerelateerde situaties op de sociale media te zetten tenzij betreffende persoon of personen hier uitdrukkelijk toestemming voor plaatsing hebben gegeven;

7. Monitoring en controle

7.1. Controle van gebruik van de ICT-faciliteiten en internetgebruik vindt slechts plaats in het kader van veiligheid en handhaving van de regels uit de Gedragscode voor de doelen genoemd bij paragraaf 1.

7.2. Ten behoeve van controle op veiligheid en de naleving van de regels worden gegevens geautomatiseerd verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten.

7.3. De Stroming houdt zich bij het controleren op het niveau van verkeersgegevens of persoonsgegevens onverkort aan de Algemene Verordening Gegevensbescherming en andere relevante wet- en regelgeving. In het bijzonder beveiligt de Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

7.4. Enkele specifieke maatregelen ter controle die de Instelling kan voeren, zijn:

- controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van filtering van de inhoud op trefwoorden. Verdachte berichten worden automatisch teruggestuurd naar de afzender;
- controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot het op basis van verkeersgegevens nagaan van de bronnen van kosten of capaciteitsvraag. Als deze websites tot grote kosten of overlast leiden, worden zij geblokkeerd of afgeknepen, zonder daarbij de vertrouwelijkheid van de inhoud van de communicatie te schenden;
- controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.

8. Rechten van de werknemer mbt persoonsgegevens

8.1. De werknemer kan zich tot het bestuur wenden met het verzoek om

- het recht op informatie over de verwerkingen;
- het recht op inzage in zijn gegevens;
- het recht op correctie van de gegevens als deze niet kloppen;
- het recht op verwijdering van de gegevens (‘het recht om vergeten te worden’);
- het recht op beperking van de gegevensverwerking;
- het recht om bezwaar te maken tegen de gegevensverwerking;

- het recht op overdracht van zijn gegevens (dataportabiliteit);
- het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming. Bij een dergelijk verzoek wordt de medewerker binnen een maand geïnformeerd over de uitvoering van het verzoek.

8.2. Het bestuur zal de werknemer geen opdrachten of dienstbevelen geven ten aanzien van privacygevoelige informatie en persoonsgegevens die in strijd zijn met de Gedragscode.

9. Consequenties van overtreding

9.1. Bij handelen in strijd met de Gedragscode of de algemeen geldende wettelijke regels, kan het bestuur afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst. Daarnaast kan het bestuur besluiten tot een al dan niet tijdelijke beperking in de toegang tot bepaalde ICT faciliteiten.

9.2. Disciplinaire maatregelen (behalve een waarschuwing) worden niet getroffen enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade. Voorts worden geen disciplinaire maatregelen getroffen zonder dat de werknemer de gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

9.3. Aanvullend op voorgaande is het mogelijk dat de Instelling bij (geautomatiseerde) constatering van overlast door een beslissing van een bevoegd persoon een tijdelijke blokkade van de betreffende faciliteit invoert. Deze blokkade zal zolang worden gehandhaafd tot aangetoond is dat de oorzaak is weggenomen. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

10. Slotbepaling

10.1. Deze Gedragscode wordt 1 x per 4 jaar of indien er tussentijds aanleiding voor is, geëvalueerd door het bestuur en andere partijen zoals de GMR..

10.2. De organisatie kan dit reglement met instemming van de GMR wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de werknemers bekendgemaakt. Het bestuur zal feedback van werknemers in overweging nemen alvorens de wijzigingen in te voeren.

10.3. In gevallen waarin de ‘Gedragscode’ niet voorziet, beslist het College van Bestuur.

Ondertekening bij indiensttreding

Ik heb de gedragscode gelezen en ga akkoord door ondertekening.

Naam: _____

Datum: _____

Handtekening: _____