Zaan Primair

Openbaar onderwijs

Zaan Primair e-mail- en internetprotocol

Voorgenomen besluit CvB: juni 2014
Advies directieberaad: september 2014
Instemming PGMR: oktober 2014

Zaan Primair e-mail- en internetprotocol

Regeling voor het gebruik van e-mail en internet.
Juni 2014

Doel van de afspraken

1.1. Deze regeling geeft de wijze aan waarop in de organisatie door medewerkers en gasten wordt omgegaan met e-mail en internetgebruik. Deze omvat gedragsregels ten aanzien van verantwoord gebruik van e-mail en internet en geeft regels over de wijze waarop controle op e-mail en internetgebruik plaatsvindt. Het protocol is opgesteld conform de Wet Bescherming

1.2. Persoonsgegevens (WBP).

Een totaal verbod op internetgebruik voor persoonlijke doeleinden is in strijd met artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM).

1.3. De controle op persoonsgegevens bij gebruik van e-mail en internet vindt plaats met als doel:

- Bewijs en archivering
- Systeem- en netwerkbeveiliging
- Bescherming van bedrijfsgeheim
- Voorkomen van negatieve publiciteit
- Tegengaan van seksuele intimidatie
- Tegengaan van “verboden gebruik”
- Kosten- en capaciteitsbeheersing

Algemene uitgangspunten

2.0 De door de organisatie aangeboden middelen voor gebruik van internet of e-mail, zoals computersystemen en netwerken worden als eigendom van de organisatie beschouwd en zijn bovenal bedoeld voor educatieve en zakelijke doeleinden.

2.1. Werknemers gaan op zorgvuldige wijze om met wachtwoorden: laten deze niet slingeren en geven ze niet af aan anderen; noch op school, noch thuis.

2.2. De controle op e-mail en internetgebruik zal overeenkomstig deze afspraak worden uitgevoerd. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het arbeidsrechtelijk kader en de Wet Bescherming Persoonsgegevens (WBP) en in overleg met de PGMR gehandeld worden.

2.3. Gegevens die tot een persoon herleidbaar zijn, zullen niet worden geregistreerd, verzameld, gecontroleerd, gecombineerd dan wel bewerkt, anders dan in dit protocol is afgesproken.

2.4. Gestreefd wordt naar een goede balans tussen controle op verantwoord e-mail en internetgebruik en bescherming van de privacy van werknemers op de werkplek.

2.5. Persoonsgegevens gerelateerd aan e-mail en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 6 maanden.

2.6. Indien dit uit een oogpunt van noodzakelijk te verrichten werkzaamheden onvermijdelijk is, is het aan het beheer van het netwerk toegestaan om persoonlijke data van gebruikers tijdelijk ontoegankelijk te maken. Anders dan in acute noodsituaties, worden gebruikers tijdig op de hoogte gebracht van deze tijdelijke ontoegankelijkheid.

2.7. De werkgever treft voorzieningen voor de positie en integriteit van de systeembeheerder en/of afdeling systeembeheer en de controle daarop.

Vanuit het oogpunt van de privacy is het belangrijk om afspraken te maken wie in welke gevallen opdracht kan geven tot de controle. Zie hiervoor Controle 5.2. Ook de geheimhoudingsplicht (art. 12, lid 2 WBP) dient ter sprake te komen in verband met de eigen integriteit van de systeembeheerder.

E-mailgebruik

3.1. Werknemers mogen:

- Het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk en mits dit gebruik tot een minimum wordt beperkt

3.2. Het versturen van e-mailberichten moet voldoen aan de volgende voorwaarden:

- Een correcte vermelding van afzender
- Het meesturen van een disclaimer
- Duidelijke onderwerp aanduiding indien het een privé-mail betreft

3.3. Het is niet toegestaan om:

- Dreigende, beledigende, seksueel getinte dan wel discriminerende berichten te versturen
- Kettingbrieven te versturen

3.4. De werkgever zal niet de inhoud van zowel persoonlijke als zakelijke e-mailberichten lezen. Gegevens omtrent het aantal e-mails, e-mailadressen en andere data hieromtrent worden wel geregistreerd, voor zover dit vereist is i.v.m. wettelijke of contractuele verplichtingen (Telecommunicatiewet) Op incidentele basis kan vanwege een zwaarwichtige reden controle plaatsvinden. Hiervan wordt melding gemaakt bij de PGMR.

Internetgebruik

4.1. Werknemers mogen:

- Het internetsysteem voor persoonlijke doeleinden gebruiken mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk en mits dit gebruik tot een minimum wordt beperkt

4.2. Het is niet toegestaan om:

- Bewust sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten
- Te handelen in goederen en diensten vanuit privé belang
- Te gokken
- Op internet in strijd met de wet of onethisch te handelen
- Software en applicaties, zonder overleg met de ICT-afdeling, te installeren

4.3. De werkgever zal geen persoonsgegevens over internetgebruik, zoals tijdsbesteding en bezochte sites, registreren en/of controleren. Op incidentele basis kan vanwege een zwaarwichtige reden controle plaatsvinden. Hiervan wordt melding gemaakt bij de PGMR.

Controle

5.1. Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een werknemer of een groep werknemers ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaats vinden.

- Conform de bedrijfsregels laat de bestuurder de bovenschoolse ICT-coördinator een kopie van de zakelijke e-mailberichten maken met als doel bewijs en/of archivering
- Voor het tegengaan van virussen en andere schadelijke programma's, in het kader van systeem- en netwerkbeveiliging, wordt het e-mail en internetgebruik op geautomatiseerde wijze gecontroleerd
- Medewerkers die spam ontvangen, moeten dit melden via spam@zaanprimair.nl
- Controle op het uitlekken van bedrijfsgeheimen vindt plaats op basis van steekproefsgewijze content filtering. Een verdacht bericht wordt apart gezet voor nader onderzoek
- Controle in het kader van het voorkomen van negatieve publiciteit vindt plaats op basis van content filtering. Verdachte berichten worden geautomatiseerd teruggestuurd naar de afzender en "verboden" sites geblokkeerd
- Controle in het kader van het tegengaan van seksuele intimidatie vindt op geautomatiseerde wijze plaats. Verdachte berichten worden geautomatiseerd terug gestuurd naar de afzender
- Controle in het kader van het tegengaan van "verboden gebruik" vindt in beginsel geanonimiseerd en slechts steekproefsgewijs plaats

- Controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeersgegevens (tijd, hoeveelheid, omvang, en dergelijke)

5.2. Controle beperkt zich in principe tot verkeersgegevens van het gebruik van e-mail en internet. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats. Hiervan wordt melding gemaakt bij de PGMR.
5.3. "Verboden" e-mail- en internet gebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Overige controle vindt slechts steekproefsgewijs plaats.
5.4. Werknemers ten aanzien van wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken.
5.5. E-mailberichten van (G)MR-leden, bedrijfsartsen en andere medewerkers met een vertrouwensfunctie zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het berichtenverkeer.

Rechten van de betrokkenen

6.1. De werkgever informeert de werknemers voorafgaand aan de invoering van de regeling over controle op e-mail- en internetgebruik, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling (zie artikel 33 WBP)
6.2. Inzagerecht: De werknemer heeft het recht de over hem of haar geregistreerde data in te zien. Verzoeken om inzage worden binnen 20 werkdagen ingewilligd. (zie artikel 35 WBP)
6.3. Kopierecht: De werknemer heeft het recht van de over hem of haar geregistreerde data een kopie te ontvangen binnen 20 werkdagen.
6.4. Correctierecht: De werknemer heeft het recht om feitelijk onjuiste gegevens uit de geregistreerde data te (laten) vervallen of aan te vullen. Over verzoeken van correctie of aanvulling wordt binnen 20 werkdagen beslist. Indien een verzoek tot correctie of aanvulling wordt ingewilligd wordt de correctie terstond uitgevoerd. (zie artikel 36 WBP)
6.5. Verwijderingsrecht: De werknemer heeft het recht om de over hem of haar geregistreerde data die niet (langer) ter zake doen, of in strijd zijn met dit protocol of een wettelijk voorschrift te verwijderen en te vernietigen. Over een verzoek om verwijdering en vernietiging wordt binnen 20 werkdagen beslist. Indien een dergelijk verzoek wordt ingewilligd, vindt de verwijdering en vernietiging terstond plaats. (zie artikel 40 WBP)

Sancties

7.1. Bij handelen in strijd met deze regeling, het bedrijfsbelang of de algemeen geldende normen en waarden voor het gebruik van het netwerk, internet en e-mail, kunnen afhankelijk van de aard en de ernst van de overtreding maatregelen worden getroffen.
7.2. Voor medewerkers betreft dit disciplinaire en arbeidsrechtelijke maatregelen zoals berisping, overplaatsing, schorsing of beëindiging van de arbeidsovereenkomst.
7.3. Voor gasten betreft dit maatregelen als tijdelijke of permanente ontzegging van de toegang het netwerk of internet.

Slotbepaling

8.1. Dit protocol is beleid als bedoeld in artikel 12 lid *m, n* van de Wet op de medezeggenschap en zal door de werkgever c.q. het bestuur, aan de PGMR worden toegezonden. De werkgever kan deze regeling met instemming van de PGMR wijzigen. Deze wijzigingen worden schriftelijk vastgelegd en voorafgaand aan de invoering aan de werknemers bekend gemaakt.
8.2. Dit protocol laat elke uit wet, cao of andere geldende regeling voortvloeiende bevoegdheid of voorziening voor de PGMR onaangetast.
8.2.Deze regeling treedt in werking op……. Dit protocol wordt indien nodig, maar tenminste eens per vier jaar geëvalueerd en bijgesteld.
8.3. Deze regeling is tot stand gekomen in overleg met en met instemming van de PGMR.