PROTOCOL EMAIL, NETWERK EN INTERNETGEBRUIK

OZHW voor PO en VO

Onderwijsgroep
Zuid-Hollandse Waarden
voor primair en voortgezet onderwijs

Dit protocol vervangt het eerdere email, netwerk en internetgebruik van OZHW voor PO en VO en de scholen die tot haar scholengroep behoren. Het protocol is in het kader van het vaststellen van het sociaal veiligheidsbeleid na instemming van de (G)MR op [datum] door het bestuur vastgesteld op [datum].

Versiebeheer

Versie	Datum	Omschrijving	Opmerking
0.1	Jan.2020	Opgesteld door P. Schijff	E-mail, netwerk en internetgebruik aangepast aan AVG

Akkoord

Naam	Functie	Datum	Handtekening

Protocol email, netwerk en internetgebruik

Artikel 1 DEFINITIES, DOEL EN WERKING

1. Dit protocol bevat een regeling voor het gebruik van het computernetwerk, e-mail en internet door medewerkers en leerlingen van OZHW, alsmede voor derden die gebruik maken van het computernetwerk, e-mail en internet van OZHW.
2. Deze regeling omvat gedragsregels voor verantwoord gebruik van het computernetwerk, e-mail en internet en geeft regels over de wijze waarop controle plaatsvindt
3. Het protocol is opgesteld conform de Algemene Verordening Gegevensbescherming (AVG) van 25 mei 2018, als opvolger van de Wet Bescherming Persoonsgegevens.
4. Het protocol bevat regels voor en afspraken over het computergebruik door medewerkers en leerlingen van OZHW, alsmede voor derden die gebruik maken van het computernetwerk, e-mail en internet van het OZHW (hierna gebruikers genoemd) en over de manier waarop OZHW omgaat met het registreren, verzamelen en monitoren van tot een persoon herleidbare data inzake het gebruik van hardware, software, e-mail en internet. Doelstelling hiervan is een goede balans te vinden tussen een verantwoord gebruik van internet en e-mail en de bescherming van de privacy van gebruikers op de werkplek.
5. Onverantwoord gebruik is gebruik dat tegenstrijdig is aan de doelstelling en identiteit van de school, zowel in persoonlijk gebruik als in relatie tot anderen binnen of buiten de school. Hierbij wordt in het bijzonder gedacht aan illegale toepassingen van bestanden, godslasterlijke, beledigende, aanstootgevende, gewelddadige, racistische, discriminerende, intimiderende, pornografische toepassingen, zinloos tijdverdrijf en toepassingen die strijdig zijn met de wet of als onethisch aan te merken zijn.
6. De controle op persoonsgegevens bij gebruik van het computernetwerk, e-mail en internet vindt plaats met als doel:
    a. systeem- en netwerkbeveiliging;
    b. tegengaan van onverantwoord gebruik.
7. Het protocol geldt voor alle gebruikers die op welke wijze dan ook gebruik maken van het netwerk van het OZHW.
8. Het protocol behelst e-mail, netwerk- en internetgebruik. Hieronder wordt verstaan ieder gebruik van de door het OZHW geboden faciliteiten: het gebruik van het netwerk van OZHW, het gebruik van het zakelijke e-mailadres en het gebruik maken van toegang tot internet.

Artikel 2 ALGEMENE UITGANGSPUNTEN

1. 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. Persoonsgegevens zullen alleen gebruikt worden voor het doel waarvoor ze verzameld zijn passend binnen de Algemene Verordening Gegevensbescherming.
3. Het registreren van gegevens die tot een persoon herleidbaar zijn, wordt tot het minimum beperkt. Hierbij wordt gestreefd naar een maximale bescherming van de privacy van de gebruikers op de werkplek.
4. 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.
5. Persoonsgegevens over gebruik van het computernetwerk, e-mail en internet worden niet langer bewaard dan noodzakelijk.
6. Met het opslaan van de e-mails worden ook persoonsgegevens verzameld. Het ligt in de aard van e- mail dat de inhoud ook bijzondere persoonsgegevens kan bevatten. Op verzoek kunnen e-mails met bijzondere persoonsgegevens eerder worden vernietigd.
7. De schoolleiding treft voorzieningen voor de positie en integriteit van de systeembeheerder. Dit wordt geconcretiseerd door de systeembeheerder alleen technisch verantwoordelijk te laten zijn en dit laat onverlet het bepaalde in artikel 6.5.

Artikel 3 ALGEMENE BEPALINGEN t.a.v. GEBRUIKERS

1. Alle medewerkers en leerlingen van OZHW hebben toegang tot het computernetwerk. Ook derden kan toegang worden verschaft tot het netwerk.
2. De eerste keer dat iemand gebruik maakt van het computernetwerk wordt beschouwd als de totstandkoming van een overeenkomst tussen OZHW en de gebruiker, waarbij de gebruiker instemt met de in dit protocol verwoorde regels en afspraken.
3. Het recht om gebruik te maken van het computernetwerk vervalt zodra iemand geen medewerker of leerling meer is van OZHW zoals beschreven in artikel 3.1.
4. Het computernetwerk kan door gebruikers worden benaderd op daartoe ingerichte werkplekken alsmede via de eigen laptop door middel van gebruikmaking van het draadloze netwerk.

Artikel 4 EMAIL EN INTERNETGEBRUIK GEBRUIKERS

1. Alle gebruikers van het netwerk mogen het e-mailsysteem en de toegang tot internet kortstondig, beperkt en incidenteel gebruiken voor niet-zakelijk (ofwel persoonlijk) verkeer voor het ontvangen en versturen van persoonlijke mailberichten, zowel intern als extern, mits dit niet storend is voor de dagelijkse werkzaamheden, voor anderen en het de goede werking van het netwerk niet verstoort en mits in overeenstemming met het bepaalde in deze regeling.
2. Het recht van de gebruiker om persoonlijke e-mailberichten te ontvangen en te versturen is gebonden aan de voorwaarde dat het niet is toegestaan dreigende, seksueel intimiderende, racistische dan wel andere berichten te versturen die in strijd zijn met de algemeen geldende normen en waarden en de huisregels van OZHW.
3. Het ontvangen en verzenden van persoonlijke e-mail dient voorts te geschieden met inachtneming van het bepaalde in artikel 1.
4. OZHW behoudt zich het recht voor de toegang tot bepaalde sites te beperken en/of te verbieden. Met name sites met een pornografische, racistische, discriminerende of op entertainment gerichte inhoud zullen worden geweerd.
5. Medewerkers van de afdeling ICT van OZHW zullen in principe niet de inhoud van persoonlijke en van zakelijke e-mailberichten lezen. Gegevens over het aantal mails, de e-mailadressen en andere data hieromtrent worden wel geregistreerd, voor zover dat vereist is in verband met wettelijke of contractuele verplichtingen. Dit laat onverlet dat controles op

incidentele basis (steekproef) of vanwege een zwaarwichtige reden kunnen plaatsvinden. Hiervan wordt altijd vooraf melding gemaakt bij de directie door (een medewerker van) de afdeling ICT.

6. Voor het gebruik van e-mail geldt verder:
    a) Alleen het e-mailadres dat door de organisatie is toegewezen aan de gebruiker mag worden gebruikt. Bij communicatie via e-mail moet herleidbaar zijn wie de afzender is.
    b) De afzender is verantwoordelijk voor een juiste adressering van zijn of haar informatie.
    c) De normale gedragsregels, die gelden voor schriftelijke correspondentie (zoals correct taalgebruik) zijn ook van toepassing op e-mail en andere toepassingen (zoals nieuwsgroepen).
    d) Alle regels voor elektronische informatie gelden tevens voor bijlagen.
    e) Verzending van vertrouwelijke informatie of gevoelige informatie via e-mail is niet toegestaan.

Artikel 5 GEDRAGSREGELS / BEWUST ZIJN VAN DE RISICO'S VAN INTERNETGEBRUIK

1. Het internet is een open infrastructuur die voor iedereen toegankelijk is. De gebruiker moet zich ervan bewust zijn dat de betrouwbaarheid (beschikbaarheid, integriteit en exclusiviteit) van informatie op het internet niet altijd gewaarborgd is en dat alle activiteiten die de gebruiker op internet ontplooit, bekeken en vastgelegd kunnen worden door vele partijen. Berichtgeving die gevoelige informatie of persoonsgegevens bevat, zoals bedoeld in de Algemene Verordening Gegevensbescherming (AVG), mag niet per e-mail of internet worden verzonden, tenzij dit gebeurt via een veilige, gecodeerde verbinding.
   Verder vraagt de kwetsbaarheid van de infrastructuur van internet om speciale aandacht op tenminste de volgende punten:
    a) gebruikersnaam (inlognaam) en wachtwoord zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven; de geregistreerde gebruiker is verantwoordelijk voor alle acties die met behulp van zijn/haar gebruikersnaam worden uitgevoerd;
    ~~b)~~ het downloaden en uploaden applicaties is niet toegestaan, tenzij vooraf schriftelijke toestemming is verleend door de verantwoordelijke en het hoofd van de afdeling ICT.
2. Onbedoelde inbreuken op beveiliging, van binnenuit of vanuit de buitenwereld, dienen aan een medewerker van de afdeling ICT gemeld te worden, via Security@ozhw.nl.
3. Het is in het bijzonder niet toegestaan op internet:
    a) sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
    b) pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal dat op de een of andere manier in strijd is met de grondslagen van OZHW te bekijken, te uploaden, downloaden of te verspreiden;
    c) spelletjes en muziekbestanden te uploaden, downloaden, uit te wisselen of uit te voeren, te winkelen, te gokken, deel te nemen aan kansspelen en/of chat-/babbelboxen te bezoeken, tenzij zoiets past in het kader van onderwijsactiviteiten;
    d) zich ongeoorloofd toegang te verschaffen tot niet-openbare bronnen op het netwerk van OZHW of het internet;
    e) opzettelijk informatie, waartoe men via het netwerk en/of internet toegang heeft verkregen, zonder toestemming te veranderen of te vernietigen.

Indien ongevraagd informatie wordt aangeboden die voldoet aan bovengenoemde beschrijvingen dient dat aan een medewerker van de afdeling ICT gemeld te worden. Het is bovendien niet toegestaan om door middel van e-mail:

a) berichten anoniem of onder een fictieve naam te versturen; dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en ketting e-mailberichten te verzenden of door te sturen;
b) iemand elektronisch lastig te vallen.

Het is ook niet toegestaan op een andere manier op internet handelingen te verrichten die in strijd zijn met de wet of onethisch te handelen.

4. De gebruiker verplicht zich de computer waarop hij/zij gewerkt heeft te blokkeren of af te sluiten teneinde het ongeautoriseerde gebruik van het netwerk te voorkomen. Dit geldt ook voor laptops in eigendom van een gebruiker.
5. Het is niet toegestaan om foto's, video's of ander materiaal van op school werkzame personen, leerlingen of andere bij de school betrokkenen via elektronische informatie- en communicatiemiddelen bekend te maken. Voor het bekend maken van foto's waarop personen zijn afgebeeld, is voorafgaande toestemming van betrokkene of diens wettelijke vertegenwoordiger vereist.

Artikel 6 CONTROLE

1. Controle op gebruik van elektronische informatie- en communicatiemiddelen vindt slechts plaats in het kader van in artikel 1 genoemde doelen.
2. De schoolleiding informeert de gebruikers voorafgaand aan de invoering van de regeling over controle op elektronische informatie- en communicatiemiddelen, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.
3. Niet toegestaan gebruik van elektronische informatie- en communicatiemiddelen wordt zo veel mogelijk technisch onmogelijk gemaakt.
4. Controle vindt in beginsel steekproefsgewijs plaats.
5. Als een lid van de schoolleiding of de systeembeheerder merkt, of er op geattendeerd wordt, dat het email- en internetgedrag of het gebruik van het computernetwerk van een gebruiker niet binnen deze kaders verloopt, wordt de gebruiker hier op gewezen en wordt een controle van zijn e-mail en internetacties door bevoegde personen als mogelijkheid genoemd.
6. Elektronische informatie- en communicatieberichten van de (bovenschoolse) schoolleiding, bestuursleden, vertrouwenspersonen en andere medewerkers met een vertrouwensfunctie, gecommuniceerd in het kader van hun functie, zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle bij een ernstig vermoeden van misbruik.
7. De geanonimiseerde rapportage wordt verstrekt aan de schoolleiding en aan het hoofd ICT. De schoolleiding kan naar aanleiding van deze rapportage vragen om een gepersonaliseerde rapportage.
8. Indien een gebruiker of een groep gebruikers ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden. De schoolleiding meldt dit aan het bestuur.
9. Het bestuur geeft indien nodig aan het hoofd ICT de opdracht om de elektronische informatie- en communicatiemiddelenacties van de betrokkene na te gaan.
10. Het hoofd ICT brengt hiervan schriftelijk verslag uit aan het bestuur.

11. Gebruikers bij wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door de leidinggevende of de schoolleiding op hun gedrag aangesproken.
12. Binnenkomend en e-mailverkeer wordt zo goed mogelijk gecontroleerd op virussen en soortgelijk ongerief. Indien een e-mailbericht een virus bevat dan wordt dat bericht automatisch tegengehouden. Verzender en ontvanger worden zo mogelijk daarover ingelicht. Indien desondanks een e-mail wordt ontvangen dat mogelijk een virus bevat, dan dient de ontvanger zo snel mogelijk contact op te nemen met de afdeling ICT van OZHW.
13. Voor zover noodzakelijk worden derden ingeschakeld bij onderzoek en controlewerkzaamheden.

Artikel 7 SANCTIES

1. In eerste instantie geldt hier de gedragscode van OZHW.
2. Bij handelen in strijd met deze regeling, het schoolbelang 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:
    a) Voor medewerkers van OZHW gaat het eventueel om disciplinaire en arbeidsrechtelijke maatregelen zoals berisping, schorsing of beëindiging van de arbeidsovereenkomst.
    b) Voor leerlingen zijn maatregelen denkbaar als tijdelijke of permanente ontzegging van de toegang tot het netwerk of tot internet.
    c) Daarnaast kunnen voor leerlingen ook maatregelen getroffen worden zoals schorsing op grond van overtreding van de huis- en orderegels als bedoeld in het schoolreglement.
    d) De meest vergaande sanctie voor leerlingen is verwijdering van de school. Aan derden kan de toegang tot het netwerk worden ontzegd.
3. Het is medewerkers van de afdeling ICT toegestaan om verboden, niet-zakelijk of aanstootgevend materiaal, bij wijze van voorlopige maatregel, direct te blokkeren.

Artikel 8 RECHTEN VAN DE GEBRUIKERS

1 Op grond van de Algemene Verordening Gegevensbescherming (AVG) hebben betrokkenen ten aanzien van de verwerking van persoonsgegevens de navolgende rechten. OZHW heeft deze rechten vastgelegd in het Protocol Inzageverzoek OZHW d.d. 28 mei 2019, te weten:
- Inzagerecht:
- Recht op dataportabiliteit;
- Kopierecht:
- Recht om vergeten te worden / Verwijderingsrecht;
- Recht om minder gegevens te verwerken;
- Bezwaarrecht;
- Correctierecht.