IT-REGLEMENT

ARTIKEL 1 **BEGRIPSBEPALING**
In deze regeling wordt verstaan onder

- **De instelling**: Stichting Scholen aan Zee en alle daaronder vallende locaties.
- **IT-faciliteiten**: het computernetwerk en de computers van de instelling en alle hiermee verbonden IT-apparatuur in eigendom en/of onder beheer van de instelling en alle hierop geïnstalleerde software en aangeboden IT-diensten. Ook eigen apparatuur (pc's, laptops, tablets, smartphones, etc.) die wordt verbonden met het computernetwerk van de instelling en/of van de IT-diensten van de instelling gebruik maakt, valt hieronder.
- **Communicatieplatformen**: digitale communicatiemiddelen waaronder e-mail, fora, nieuwsgroepen, chat, Teams, sociale media en internet(sites).
- **Beheerder**: afdeling IT van Scholen aan Zee.
- **Gebruiker:** ieder die het recht heeft gebruik te maken van de IT-faciliteiten van de instelling.

ARTIKEL 2 **TOEGANG**
Toegang tot de faciliteiten verkrijgt de gebruiker via de locatie waar hij werkzaam is of via een web-based of virtueel privénetwerk buiten de instelling.

ARTIKEL 3 **COMMERCIEEL GEBRUIK**
Het is niet toegestaan om de IT-faciliteiten te gebruiken voor privédoeleinden met een commercieel karakter. Het is onder andere niet toegestaan je Scholen aan Zee laptop te gebruiken bij een tweede werkgever.

ARTIKEL 4 **TOEGANG TOT HET NETWERK**
De gebruiker mag alleen met een geldige toegangscode gebruik maken van het netwerk van de instelling. Een toegangscode bestaat uit een combinatie van gebruikersnaam, wachtwoord en eventuele aanvullende authenticatiemiddelen zoals een smartcard of token. De toegangscode is strikt persoonlijk en niet overdraagbaar. De gebruiker is verantwoordelijk voor het gebruik van de gebruikersnaam en het wachtwoord en de eventuele smartcard of token. De gebruiker dient deze daarom geheim te houden. De gebruiker dient een niet-vanzelfsprekend wachtwoord te kiezen. De gebruiker moet bij vaststellen van misbruik van zijn gebruikersnaam, wachtwoord, eventuele smartcard of token direct contact opnemen met de beheerder. Het is niet toegestaan andermans gebruikersnaam, wachtwoord, eventuele smartcard of token en/of e-mailadres te gebruiken of proberen deze te achterhalen. Zie ook de procedure beveiligingsincidenten en datalekken in het informatie beveiliging en privacy beleid.

ARTIKEL 5 **IDENTITEITSVERVALSING**
Het inloggen onder een valse naam, het vervalsen van adresgegevens of het anderszins veranderen van gebruikersgegevens met als doel de identiteit van de zender te verbergen of de regels van dit reglement te omzeilen, is niet toegestaan.

ARTIKEL 6 **BEVEILIGING**
Iedere poging om 'geweigerde dienst' authenticatie of een andere beveiligingsmaatregel te doorbreken en iedere niet geautoriseerde poging om toegang te krijgen tot een IT-faciliteit is niet toegestaan. Het is ook niet toegestaan om zich al dan niet door middel van het doorbreken of kraken van een beveiligingscode, ongeoorloofd de toegang te verschaffen tot andermans gegevens, bestanden en/of computersystemen.
Een systeem waarop de gebruiker heeft ingelogd moet worden afgesloten bij het einde van het gebruik. Een systeem waarop is ingelogd wordt te allen tijde door de gebruiker vergrendeld bij het onbeheerd achterlaten van dit systeem. Zie ook Wetboek van Strafrecht, Boek II, Titel V, Artikel 138ab
Wetsartikel computervredebreuk.

ARTIKEL 7 **GEBRUIK VAN COMMUNICATIEPLATFORMEN**

Gedrag middels communicatieplatformen met gebruikmaking van de IT-faciliteiten en/of gericht jegens gebruikers van de instelling, de instelling zelf of derden, dat leidt tot overlast, onwettig is of schade aanricht door o.a. bedreiging, intimidatie, laster, discriminatie, obsceniteit, privacyschending of softwarepiraterij, is niet toegestaan. Gebruikers dienen zich ervan bewust te zijn dat gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar kunnen zijn, ook na verwijdering van het bericht. Men is in alle gevallen zelf verantwoordelijk voor de inhoud die men publiceert via deze communicatieplatformen. Op de door de instelling geïnitieerde communicatieplatformen is het voor daartoe geautoriseerde medewerkers van de instelling alleen toegestaan om aan het onderwijsproces gerelateerde informatie te publiceren. Zie ook het social media protocol.

ARTIKEL 8 **DE WIJZE VAN CONTROLE OP HET GEBRUIK VAN IT-FACILITEITEN**

Controle op het gebruik van IT-faciliteiten vindt plaats op last van het college van bestuur binnen de kaders van dit reglement en de op dit reglement van toepassing zijnde wettelijke bepalingen. Controle richt zich op:

- het tegengaan van virussen en andere schadelijke programma's: in het kader van systeem- en netwerkbeveiliging middels geautoriseerde controle van e-mail en internetgebruik;
- gedrag zoals aangegeven in artikel 7, in beginsel anoniem en steekproefsgewijs, tenzij in nadrukkelijke opdracht van het college van bestuur.

Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een gebruiker c.q. een groep gebruikers ervan wordt/worden verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode op last van het college van bestuur, daartoe eventueel geadviseerd door de beheerder, gerichte controle plaatsvinden.
Controle beperkt zich in principe tot verkeersgegevens van het gebruik van IT-faciliteiten. Alleen bij zwaarwegende redenen, te bepalen door het college van bestuur, eventueel op advies van de beheerder, vindt er controle op de inhoud plaats.
Het gebruik van IT-faciliteiten door leden van de medezeggenschapsraad en medewerkers met een vertrouwensfunctie (vertrouwenspersonen) is in principe uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het berichtenverkeer en bij een ernstig vermoeden van misbruik zoals bedoeld in art. 4 t/m 7 van dit reglement.

ARTIKEL 9 **ANTIVIRUS**

Het is verboden om computervirussen te activeren en/of te verspreiden. Gebruikers zijn verplicht een gesignaleerd virus te melden bij de beheerder.

ARTIKEL 10 **SCHENDING VAN COPYRIGHT EN INTELLECTUEEL EIGENDOM**

Gebruik van de IT-faciliteiten waardoor schending van copyright en/of overig intellectueel eigendom plaatsvindt, bijvoorbeeld door het plaatsen van software, muziek, boeken etc. op het netwerk, is niet toegestaan.
Eventuele auteursrechten op informatie die met behulp van de faciliteiten en/of voorzieningen ter beschikking worden gesteld en/of worden verspreid, worden niet uitgeoefend jegens de instelling. Indien andersluidende bepalingen zijn opgenomen in de informatie zal de informatie onmiddellijk en zonder verdere opgave worden verwijderd.

ARTIKEL 11 **GEGEVENSOPSLAG**

Gebruikers kunnen data van de instelling opslaan op hun privéruimte (OneDrive), of in één van de onderwijs- of bedrijfsapplicaties zoals de elektronische leeromgeving, het leerlingvolgsysteem of het Enterprise resource planningssysteem. De gebruiker dient zich te realiseren dat alle content opgeslagen op een andere wijze dan hiervoor aangegeven, door de instelling niet in de back-up wordt meegenomen. Er mag geen data van de instelling op opslagmedia van randapparatuur (pc's, laptops, tablets, smartphones, etc.), eigen apparatuur of apparatuur van derden worden opgeslagen. De gebruiker exporteert niet onnodig gegevens uit een bronsysteem. De gebruiker bewaart en muteert gegevens zoveel mogelijk op de server of binnen de betreffende applicatie.

ARTIKEL 12 **PRIVACY**

Zie privacyreglement leerlingen en medewerkers.

ARTIKEL 13 **ONREGLEMENTAIR GEDRAG**

Voorbeelden van onreglementair gedrag:

- gebruik van spelletjes;
- storend gebruik van geluid;
- gebruikmaken van communicatieplatformen die niet in relatie staan met de (opgedragen) onderwijs of bedrijfsactiviteiten;
- delen van vertrouwelijke of persoonlijke informatie;
- delen van informatie die betrokkenen schaadt;
- publiceren van foto-, film- of geluidsopnamen van instelling-gerelateerde situaties, medewerkers of (mede)leerlingen tenzij betrokkenen hier uitdrukkelijk toestemming voor hebben gegeven;
- medewerkers en leerlingen gaan alleen op communicatieplatforms van Scholen aan Zee functionele digitale connecties aan. Medewerkers gaan dus in functie geen digitale relaties aan met leerlingen buiten werksituaties. Zie ook het social media protocol.
- het plaatsen van niet aan het onderwijsproces gerelateerde informatie op door de instelling geïnitieerde communicatieplatformen;
- onnodig bezet houden van hardware en randapparatuur;
- racistische uitingen;
- seksistische uitingen;
- schelden;
- pornografie bekijken dan wel verspreiden;
- illegaal kopiëren (en of downloaden) van bijvoorbeeld (onderwijs)software, videofilms, spelletjes, muziek en materiaal waarop een copyright van toepassing is;
- hacken;
- gegevensmanipulatie;
- verspreiding van virussen en illegale software;
- e-mailbommen/junkmail verspreiden;
- (D)DoS aanvallen uitvoeren;
- opzettelijk beschadigen van hardware en randapparatuur;
- installatie/de-installatie van software.

Waargenomen activiteiten dienen door de gebruiker te worden gemeld bij de beheerder of degene die namens hem optreden.

ARTIKEL 14 **SANCTIES**

Gebruikers van wie geconstateerd is dat zij zich niet aan de regels genoemd in dit reglement houden worden zo spoedig mogelijk door het college van bestuur, de directie of management op hun gedrag aangesproken. De inhoud van het gesprek wordt schriftelijk bevestigd. In het gesprek wordt aandacht besteed aan de aanleiding, waarneming of constatering en de afspraken en/of maatregelen. Dit laatste kan bijvoorbeeld vergoeding van de schade en het opheffen van de blokkering van het account betreffen. Na een eerste waarschuwing volgen bij een volgende overtreding disciplinaire maatregelen waarvan de zwaarste verwijdering van de leerling is of ontslag van een werknemer. Als er sprake is van een ander strafbaar feit kan het college van bestuur verplicht aangifte doen bij de officier van justitie/ambtenaar van politie. Bij handelen in strijd met de regels vastgelegd in dit reglement beslist uiteindelijk het college van bestuur over de te nemen (disciplinaire) maatregelen.

ARTIKEL 15 **BEWAARTERMIJN**

Met betrekking tot artikel 14 worden persoonsgegevens over e-mail- en internetgebruik niet langer bewaard dan noodzakelijk is in het kader van onderzoek en eventueel te treffen maatregelen door het college van bestuur jegens een gebruiker. De minimale periode is echter altijd een half jaar.

ARTIKEL 16 **AANSPRAKELIJKHEID**

- De gebruiker is aansprakelijk, wanneer er door opzettelijk handelen of nalaten of bewuste roekeloosheid schade ontstaat aan of gebruikmakend van de IT-faciliteiten. Bewuste roekeloosheid betekent, dat de gebruiker overgaat tot risicovol gedrag, terwijl hij/zij zich bewust is van het risico dat hij/zij neemt.
- De gebruiker dient deze schade aan de instelling te vergoeden.

ARTIKEL 17 **ONVOORZIENE OMSTANDIGHEDEN**

In omstandigheden waarin dit reglement niet voorziet, beslist het college van bestuur.