

ICT-Gedragscode voor Stichting Sterk Regionaal Onderwijs (SRO)

Instemming GMR: 17 maart 2026

Eerstvolgende evaluatie: maart 2027

1. Doel en uitgangspunten

Binnen SRO werken we met moderne digitale middelen: computers, e-mail, internet, applicaties, lesmateriaal en AI-tools. Daarmee kunnen we ons werk goed en efficiënt doen. Deze gedragscode helpt ons om **verantwoord, veilig en bewust** met die middelen om te gaan — met respect voor elkaar en voor privacy.

We werken vanuit **vertrouwen, professionaliteit en verantwoordelijkheid**.

Deze gedragscode is geen controlelijst, maar een kader voor professioneel handelen. De afspraken gelden voor iedereen die voor of binnen SRO werkt, inclusief tijdelijke medewerkers, stagiairs en externe partners.

Onze uitgangspunten zijn:

- We beschermen persoonsgegevens en vertrouwelijke informatie.
- We gaan zorgvuldig om met bedrijfsmiddelen.
- We zijn ons bewust van onze digitale voetafdruk.
- We vertrouwen op elkaars professionele oordeel.

2. Vertrouwen en verantwoordelijkheid

Iedere medewerker is zelf verantwoordelijk voor het veilige en juiste gebruik van de middelen die SRO ter beschikking stelt.

We gaan zorgvuldig om met de informatie van leerlingen, collega's en ouders, en gebruiken ICT op een manier die past bij onze professionele rol.

Een beperkt privégebruik van e-mail of internet is toegestaan, zolang dit het werk niet belemmert of risico's veroorzaakt.

Wanneer je privéapparaten gebruikt (zoals laptop of telefoon), zorg dan zelf voor goede beveiliging: een pincode of wachtwoord, actuele software en antivirus.

Leen geen werkapparaten uit aan anderen en gebruik geen onbeveiligde opslagdiensten (zoals privéclouds of USB-sticks).

Twijfel je of iets veilig of verstandig is? Vraag advies bij ICT of je leidinggevende.

Wij werken op basis van vertrouwen: **verantwoordelijkheid is de norm, niet controle**.



3. Veilig omgaan met informatie en middelen

Informatie en gegevens

- Sla gegevens uitsluitend op in de goedgekeurde SRO-bronsystemen, zoals magister en Microsoft 365.
- Deel vertrouwelijke informatie alleen met geautoriseerde collega's of partners.
- Verstuur geen persoonsgegevens via onbeveiligde kanalen.
- Verwijder documenten die niet meer nodig zijn, en vernietig papieren met persoonsgegevens.

Apparaten

- Vergrendel je computer (Windows+L) wanneer je weggaat.
- Meld verlies of diefstal van apparaten direct bij de ICT-servicedesk.
- Gebruik sterke wachtwoorden of wachzinnen, deel deze nooit en wijzig ze periodiek.
- Bewaar wachtwoorden veilig, bij voorkeur in een wachtwoordmanager.

Software en digitaal lesmateriaal

- Installeer alleen software of apps met geldige licenties en na goedkeuring.
- Vraag bij nieuw digitaal lesmateriaal of apps altijd na of persoonsgegevens worden verwerkt.
- Gebruik alleen diensten waarvoor een verwerkersovereenkomst is afgesloten.

Datalekken

Ontdek je een mogelijk beveiligingsincident of datalek? Meld dit direct bij je leidinggevende of ICT. Snel handelen voorkomt schade voor betrokkenen en voor de organisatie.

4. Digitale “omgangsvormen” in gebruik E-mail en internet

Gebruik de ICT-voorzieningen van SRO professioneel en zorgvuldig.

- Gebruik je schoolmail voor schoolzaken; privé-mail incidenteel is toegestaan.
- Houd communicatie beleefd en respectvol – ook online.
- Open geen verdachte bijlagen of links.
- Download geen illegale of auteursrechtelijk beschermde bestanden.

Sociale media

Sociale media zijn waardevolle communicatiemiddelen, maar vereisen bewust gebruik.

- Wees je bewust dat je, ook online, SRO vertegenwoordigt.
- Deel geen vertrouwelijke informatie of beeldmateriaal zonder toestemming.
- Plaats geen berichten die aanstootgevend, discriminerend of kwetsend zijn.
- Word niet via privéaccounts 'vrienden' met leerlingen of ouders.
- Twijfel je over een bericht? Plaats het niet.



Beeld- en geluidsmateriaal

Het gebruik van foto's, video's en geluidsopnamen van leerlingen of medewerkers is alleen toegestaan met wettelijke grondslag of toestemming van de betrokkene(n).

Controleer altijd of deze grondslag of toestemming er is.

Kunstmatige Intelligentie (AI)

AI kan helpen bij onderwijs en administratieve processen, maar vraagt om zorgvuldigheid.

- Gebruik alleen door SRO goedgekeurde en beheerde AI-tools.
- Voer nooit persoonsgegevens of vertrouwelijke informatie in AI-systemen in.
- Controleer altijd de juistheid van AI-output: jij blijft eindverantwoordelijk.
- Gebruik AI als hulpmiddel, niet als vervanging van menselijk inzicht.

5. Meldingen, controle en naleving

SRO vertrouwt op bewust gebruik van ICT. Controle is alleen aan de orde als daar een duidelijke aanleiding voor is (bijvoorbeeld een vermoeden van misbruik of een datalek). Controles worden uitgevoerd binnen de kaders van privacywetgeving en arbeidsrecht, en zoveel mogelijk geautomatiseerd en geanonimiseerd.

Bij overtreding van de gedragscode volgt eerst een gesprek gericht op herstel en bewustwording. Alleen bij herhaling of ernstige overtreding kunnen disciplinaire maatregelen worden genomen.

Iedere medewerker kan inzage vragen in over hem of haar vastgelegde gebruiksgegevens. Heb je vragen of twijfels over ICT-gebruik, meld dit dan bij je leidinggevende of Functionaris Gegevensbescherming (FG).

6. Bewustwording en evaluatie

Een gedragscode werkt alleen als we haar kennen, begrijpen en naleven.

Daarom zorgen we voor blijvende aandacht voor digitale veiligheid en privacy via trainingen en communicatie.

De gedragscode wordt jaarlijks geëvalueerd door het bestuur en de (G)MR.

In situaties waarin deze code niet voorziet, beslist de directeur-bestuurder.

Samenvattend

“We werken met vertrouwen, zorg en professionaliteit.

We beschermen informatie, respecteren privacy, en handelen online zoals we offline ook doen: verantwoordelijk en met gezond verstand.”