

Gedragcode Privacy



Ronduit

Bron

Kennisnet/ Privacy op School

Bewerkt door:

Stichting Ronduit

Versie	Status	Datum	Auteur	Omschrijving
0.91		1/6/22	Wanda Hoogerbrugge	Eerste versie
0.93	Ter controle SSC	29/8/22	Wanda Hoogerbrugge	Aanpassingen SSC verwerkt
0.94	Ter controle WN	8/9/22	Wanda Hoogerbrugge	Feedback WN verwerkt
0.95	Ter controle WN	21/9/22	Wanda Hoogerbrugge	Feedback WN verwerkt
1.0	afgerond	31/10/22	Wanda Hoogerbrugge	Ter goedkeuring CvB/ GMR
1.0	afgerond	15/12/22	Wanda Hoogerbrugge	Afstemming met AVG commissie GMR
1.1		28-01-2025	Suzanne van Gelder	Aanpassen huisstijl, toevoegen gebruik social media

Goedgekeurd/Vastgesteld door Ronduit:

Versie	Datum	Naam	Functie
1.0	19/1/23	C. Steeman (secretaris)	GMR
1.0			College van Bestuur

Inhoud

Gedragscode Privacy	4
Waar en hoe bewaar ik persoonsgegevens?	4
Hoe en wat communiceer ik online via e-mail en social media?	5
Hoe werk ik veilig (thuis)?	7
Werken op eigen device (pc, laptop, tablet, smartphone)	9
Onlineonderwijs	9

Gedragcode Privacy

Iedereen heeft het recht op bescherming van persoonsgegevens. Dat is vastgelegd in de wet. Het is daarom van belang dat alle werknemers weten hoe zorgvuldig om te gaan met de verwerking van persoonsgegevens. Door te werken volgens deze gedragscode privacy beschermen we de persoonsgegevens en creëren we een veilig werk- en schoolklimaat. Alle medewerkers van Ronduit dienen zich aan de code te houden.

De afspraken zijn verdeeld in vijf onderdelen:

1. Waar en hoe bewaar ik persoonsgegevens?
2. Hoe en wat communiceer ik online via e-mail en sociale media?
3. Hoe werk ik veilig (thuis)?
4. Wat moet ik regelen als ik werk op mijn eigen device?
5. Afstandsonderwijs

Hieronder volgen per onderdeel de belangrijkste afspraken.

Waar en hoe bewaar ik persoonsgegevens?

- Verwerk persoonsgegevens zoveel mogelijk in het Leerlingadministratiesysteem (ESIS/SCOL) of HR administratiesysteem (HR2day) en bewaar ze nooit op een USB-stick.
Leerlinggegevens worden zoveel mogelijk digitaal opgeslagen, geraadpleegd en bewerkt in het ESIS/SCOL. Dit geldt ook voor gegevens die via ouders/verzorgers en/of externen worden ontvangen. Gegevens over medewerkers worden bewaard in het HR administratiesysteem. Kijk in het hoofdstuk over bewaarplaatsen van persoonsgegevens voor de afspraken binnen Ronduit.
- Anonimiseer waar mogelijk map en file namen
Gebruik zo min mogelijk persoonsgegevens in bestands- en mapnamen.
- **Gebruik voor de verwerking van persoonsgegevens een computer die voldoet aan de beveiligingseisen van Ronduit**
Moet je (documenten met) persoonsgegevens downloaden en bewerken op je computer? Doe dit alleen op een computer (laptop, smartphone) van Ronduit. Verwijder de persoonsgegevens na gebruik van je computer. Zorg ervoor dat anderen (bijv. familieleden) niet bij jouw werkbestanden kunnen komen.
Werk je op je privé device? Klik dan in 1.4 van dit hoofdstuk om te zien aan welke eisen het device moet voldoen.
- **Formuleer gegevens die je vastlegt over een persoon zorgvuldig en professioneel**
Ouders hebben het recht om het leerlingdossier in te zien. Zorg ervoor dat de gegevens zodanig objectief en professioneel zijn geformuleerd, zodat dit direct kan worden ingezien door ouders.
- **Ga na welke afspraken er binnen de school zijn gemaakt, voordat je gegevens uitwisselt met derden.**
Wanneer je gegevens uitwisselt met collega's of andere organisaties, zoals bijvoorbeeld de logopedist, een arts, de jeugdzorg, een schoolbegeleidingsdienst of een andere school, kijk dan goed welke afspraken hierover zijn gemaakt binnen Ronduit. In de meeste gevallen is

toestemming nodig van de ouders. Zorg dat je de toestemming ook schriftelijk vastlegt, dit kan ook per mail.

Hoe en wat communiceer ik online via e-mail en social media?

Het gebruik van digitale communicatiemiddelen sluit aan bij de eigentijdse manier waarop Ronduit betrokkenen wil informeren en toegankelijk wil zijn. De scholen binnen Ronduit zorgen ook digitaal voor een veilig klimaat en communiceren met personeelsleden, leerlingen en ouders/verzorgers hoe zij dit doen.

Ronduit stelt aan alle medewerkers een mailaccount ter beschikking en een bijbehorende mailbox voor het uitoefenen van de werkzaamheden.

Het gebruik van sociale mediakanalen van Ronduit is alleen voorbehouden aan personeelsleden die hiervoor gemandateerd en geïnstrueerd zijn.

Advies wat betreft Social Media, januari 2025:

Veel scholen maken gebruik van Social Media voor PR doeleinden. Denk hierbij aan Instagram, Facebook en Tiktok.

Ons advies is om Social Media niet te gebruiken en anders geen leerlingen te online te posten. Ook niet als ouders toestemming hebben gegeven aan de school voor het plaatsen van foto's op social media. Er is namelijk geen verwerkersovereenkomst mogelijk met Meta. Je zou als school eigenlijk afspraken moeten maken met Meta over het gebruik van de content die je plaatst. Meta is namelijk de verwerker van je content die je plaatst. Meta mag daarom jouw content gebruiken voor marketingdoeleinden en uiteindelijk zelfs doorverkopen. Wij als bestuur zijn bij het plaatsen van leerlingen dus verantwoordelijk voor het eventueel verspreiden van foto's van onze leerlingen. Zelfs als je data verwijderd, heeft de verwerker Meta nog recht op een back-up van deze data. Het advies van de Autoriteit Persoonsgegevens is dan ook om geen leerlingen zichtbaar meer te plaatsen op Sociale media.

Je kunt als school natuurlijk wel leerlingen plaatsen op de [website van de school](#). Mits je hier toestemming voor hebt. Met de verwerker van de website is namelijk wel een verwerkersovereenkomst overeengekomen.

- Van de medewerkers binnen Ronduit wordt verwacht dat zij op een professionele manier communiceren en handelen, dat wil zeggen:
 - Geen eigen online communicatiemiddelen (privé e-mail, social media, Whatsapp) gebruiken voor het contact met ouders of leerlingen vanuit de rol als professional;
 - Dat de inhoud van de communicatie functioneel en professioneel moet zijn;
 - Niet op persoonlijke titel communiceren vanuit hun rol als professional;
 - Geen online discussie voeren met ouders/verzorgers of leerlingen;
 - Zich niet negatief uitlaten over de school, ouders/verzorgers of leerlingen;
 - bewaar communicatie op de daarvoor bestemde plaatsen (Bijv. Leerlingdossier in Esis)
- Maak gebruik van een link naar Office365 om persoonsgegevens uit te wisselen met collega's of verwijs naar de vindplaats (in ESIS/SCOL)
Verstuur nooit persoonsgegevens per mail, maar verstuur een link met de vindplaats. Wissel

persoonsgegevens nooit uit via een USB-stick.

- Vraag ouders om toestemming om een (privé)account aan te maken voor social media die in opdracht van de school (leerkracht) moet worden gebruikt, maar ook buiten de school om kunnen worden gebruikt
Leerlingen moeten toestemming hebben van hun ouders om een (privé)account aan te maken voor online diensten zoals Pinterest, Kahoot, etc.
- **Deel over individuele leerlingen nooit informatie via social media**
Doe dit vooral in persoon (eventueel via de telefoon). Wat je communiceert via sociale media kan makkelijk anders worden geïnterpreteerd door de lezer als je hier niet alert op bent. Het is medewerkers niet toegestaan om tijdens de lessen actief te zijn op social media.
- Gebruik de accounts die door de school worden beheerd als je met ouders of leerlingen wilt communiceren via e-mail of social media.
Privé-meningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de school en/of het bestuur. Je blijft altijd persoonlijk verantwoordelijk voor wat je deelt of publiceert.
- Wees terughoudend met 'vrienden' worden met leerlingen, oud-leerlingen en/of ouders van leerlingen op sociale media
Het lijkt vrij onschuldig, maar de kans dat er verkeerde informatie wordt gedeeld met leerlingen en ouders, bewust of onbewust, komt soms voor en heeft grote gevolgen voor de medewerker in kwestie. Zorg dat je niet in een lastige situatie belandt hierdoor.
- **Stuur geen privé berichten via het e-mailaccount van de school**
Het schoolaccount is bedoeld voor school gerelateerde berichten.
- Ga voordat je foto's of video's publiceert waar leerlingen herkenbaar op te zien zijn, na of ouders hiervoor toestemming hebben gegeven.
Ouders, maar ook medewerkers, moeten toestemming geven voor het publiceren van foto's en video's waarop leerlingen of medewerkers herkenbaar in beeld zijn gebracht. De toestemming moet schriftelijk vastgelegd zijn en men moet er jaarlijks aan worden herinnerd om de toestemming in te trekken of alsnog te verlenen. De toestemming moet ook expliciet zijn, dus er moet vastgelegd zijn voor welk doel men toestemming geeft.
Gebruik voor publicatie van foto's en video's alleen de aan school gerelateerde mediakanalen.
- **Zet e-mailadressen altijd in de BCC-regel als je naar (grote) groepen mensen een bericht verstuurt**
Zo blijven de e-mailadressen van de groepsleden afgeschermd en kunnen ze niet onbedoeld voor andere doeleinden (door anderen) gebruikt worden.
- Stuur nooit zomaar een e-mailbericht door naar derden. Overleg indien nodig met de degene van wie je het bericht hebt ontvangen
De afzender heeft de mail voor een ander persoon en met wellicht een ander doel geschreven. Door het door te sturen, kunnen anderen het bericht verkeerd interpreteren.

- Wanneer je een bericht stuurt met belangrijke en/of gevoelige informatie naar (een groep) ouders/verzorgers laat dit dan nalezen door een collega
Een foutje is snel gemaakt en bovendien kan een ander je boodschap anders interpreteren dan jij het bedoeld hebt.
- Wanneer je een bericht stuurt met belangrijke en/of gevoelige informatie naar (een groep) ouders/verzorgers laat dit dan nalezen door een collega
Een foutje is snel gemaakt en bovendien kan een ander je boodschap anders interpreteren dan jij het bedoeld hebt.

Hoe werk ik veilig (thuis)?

- Zorg er bij vertrouwelijke (telefonische) gesprekken voor dat er niet kan worden meegeluisterd
Trek je even terug als een gesprek een vertrouwelijk karakter heeft of krijgt.
- Wissel zo min mogelijk gevoelige en bijzondere persoonsgegevens uit via online bijeenkomsten (informatie over gezondheid, functioneren ed).

Dit houdt in dat je een vertrouwelijk gesprek bij voorkeur face-to-face te voert. Als er wel online gevoelige en/of bijzondere gegevens worden uitgewisseld, mag het gesprek niet worden opgenomen.

- **Bewaar laptops of tablets altijd op een veilige plek, zeker tijdens vakantieperiodes**
Maak elkaar er op attent als je een laptop of tablet onbeheerd ziet liggen. Als je computer gestolen wordt, heeft dat gevolgen voor de school en de leerling. Meld dit dus altijd direct bij je leidinggevende.
- **Klik alleen op linkjes en open alleen bijlagen in e-mails van betrouwbare afzenders en pas op met het downloaden van bestanden**
Virussen kunnen makkelijk worden binnengehaald via (phishing)mails. Het is een veelgebruikte methode om aan jouw gegevens te komen. Ook kunnen de gegevens op je computer op deze manier versleuteld worden (ransomware).
- Meld je altijd af als je de computer onbeheerd achterlaat. En zorg ervoor dat er op je werkplek geen gevoelige informatie zichtbaar of voor het grijpen ligt, ook bij de printer
Met de combinatie van de Windows- en L-toets kun je je computer eenvoudig vergrendelen (clear screen). Maak er een gewoonte van om papieren op je bureau om te draaien. Zorg dat de papieren in een afgesloten la of kast worden opgeborgen wanneer je je werkplek verlaat (clean desk). Zo voorkom je dat anderen informatie zien die niet voor hen is bedoeld.
- **Meld je af (uitloggen) van de Cloud toepassing** voordat je de toepassing afsluit. Met het kruisje afsluiten van het venster (rechtsboven) of de pc uitzetten is (vaak) niet voldoende. De volgende persoon die dezelfde computer gebruikt kan op deze manier toegang krijgen tot jouw bestanden/ informatie in de Cloud
- Veilig printen

Iedere medewerker heeft een unieke code ontvangen om veilig te kunnen printen. Deze code heeft dezelfde normering als een wachtwoord; deel deze code niet met anderen. Voor externen zijn speciale codes aangemaakt.

Laat geen afdrucken bij de printer liggen, zeker niet als er persoonsgegevens op staan. Haal overbodig geworden papieren documenten met persoonsgegevens altijd door de papierversnipperaar.

- Zet je digibord op freeze als je wachtwoorden intoetst of persoonsgegevens in je scherm ziet staan. En zorg dat niemand meekijkt als jij je wachtwoord intoetst
Voordat je het weet zien leerlingen gevoelige gegevens of kunnen ze aan de hand van je afgekeken gebruikersnaam en wachtwoord proberen in te loggen.
Zet ook de notificatie-functie van je e-mail uit, zodat er tijdens je les geen meldingen op het bord binnen komen die leerlingen kunnen zien, maar niet voor hun ogen bestemd zijn.
- Laat je wachtwoorden van ESIS/SCOL of andere systemen met persoonsgegevens niet onthouden door je internetbrowser. Schrijf je logingegevens nooit op!
Zonder dat je er erg in hebt, klik je de optie 'wachtwoord onthouden' in je browser aan. Heel makkelijk als je vaak moet inloggen, maar iemand anders kan dan dus ook inloggen.
- **Houd je logingegevens altijd voor jezelf, ook al vragen anderen aan je om ze te delen.**
Je login is in feite een sleutel om toegang te krijgen tot de informatie die alleen voor jou toegankelijk moet zijn. Daarnaast herkent het systeem jou door je login, zodat het kan bijhouden wie welke gegevens heeft toegevoegd of gewijzigd, deel ze dus nooit met anderen.
- Gebruik alleen educatieve software of apps als hiervoor een verwerkersovereenkomst is afgesloten
Het afsluiten van een verwerkersovereenkomst is een wettelijke verplichting als een leverancier ook persoonsgegevens verwerkt. Je kunt via je directeur achterhalen of de school een verwerkersovereenkomst heeft afgesloten.
- Publieke WIFI is niet veilig
Het gebruik van publieke wifi om Cloud toepassingen te benaderen wordt om die reden dan ook afgeraden. Met de vele toepassingen in de Cloud is het mogelijk om op andere locaties of met andere apparatuur te werken dan op school. Wees daarom bewust van waar je inlogt.
- Meld de volgende en soortgelijke voorvallen direct via www.hetictloket.nl in verband met de meldplicht datalekken.
 - Er zijn persoonsgegevens verloren gegaan.
 - Je laptop met persoonsgegevens is gestolen.
 - Je USB-stick met persoonsgegevens is kwijtgeraakt.
 - Je hebt een virus waardoor je niet meer bij je bestanden kunt.
 - Je logingegevens van het LAS zijn in handen van anderen gekomen (of je kunt dit niet uitsluiten).
 - Etc.

Werken op eigen device (pc, laptop, tablet, smartphone)

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor Ronduit worden uitgevoerd. De school is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de ICT middelen van de school.

De mobiele devices (smartphone, laptop, tablet) in eigendom van de medewerker kunnen gebruikt worden voor schoolwerkzaamheden indien ze voorzien zijn – indien van toepassing – van de volgende beveiligingseisen, zodat persoonsgegevens goed beschermd zijn:

- Het device is voorzien van een wachtwoord of code;
- De software wordt up-to-date gehouden door het uitvoeren van periodieke updates (minimaal maandelijks);
- Het device is voorzien van anti-virussoftware, die up-to-date wordt gehouden;
- E-mail en andere apps of online toepassingen van de school moeten afgeschermd worden met een apart wachtwoord;
- E-mail en andere apps of online toepassingen mogen niet toegankelijk zijn voor andere gebruikers;
- Wachtwoorden mogen niet in de browser worden onthouden;
- Er worden geen bestanden die persoonsgegevens bevatten lokaal op het device opgeslagen, maar alleen op de daarvoor aangewezen bewaarplaatsen van Ronduit;
- Het verwerken van persoonsgegevens van Ronduit mag niet via een openbaar Wifi-netwerk gebeuren.
- Als je huis inlogt met je office365 omgeving, dan gebruik je de online versie om bij je Outlook, PowerPoint en overige apps te komen, via <https://www.office.com>
- Vergrendel het eigen device bij het verlaten van de werkplek (windowstoets+L);
- Laat geen huisgenoten op het eigen devices werken, wanneer dit niet in een gescheiden omgeving kan worden gedaan.

Onlineonderwijs

De school kan in bepaalde situaties ervoor kiezen dat de leerlingen les krijgen via videobellen. Daarbij komen de leraren en/of leerlingen in beeld. Dit mag zonder toestemming als lesgeven op een andere manier niet kan, zoals tijdens een lockdown.

Samen willen we ervoor zorgen dat de inbreuk op de privacy zo klein mogelijk blijft. Dat doen we door onderstaande gedragsregels in acht te nemen:

- Zorg dat de software (op laptops en computers) is bijgewerkt en maak gebruik van antivirusprogramma's.

- Gebruik jouw eigen account en deel je wachtwoord nooit met anderen.
- Controleer voor aanvang of de camera, microfoon en luidspreker het goed doen.
- Maak bij voorkeur gebruik van een koptelefoon met microfoon.
- Zet tijdens de les standaard de microfoon uit. De leraar kan op afstand de microfoon aan- of uitzetten en bepaalt wie het woord krijgt.
- Kies een achtergrond uit Teams.
- Zorg voor een rustige plek in huis en dat er tijdens de les zo min mogelijk afleiding is.
- Zorg ervoor dat andere huisgenoten of bezoekers weten dat een videoles wordt gegeven en dat alles wordt uitgezonden.
- De link naar de videoles is vertrouwelijk. Laat andere mensen, vrienden of familie deze link niet gebruiken.
- De lessen mogen niet worden opgenomen. Screenshots of foto's maken is ook niet toegestaan.
- Het opnemen van lessen kan in uitzonderlijke situaties plaats vinden, na toestemming van de directeur. Dit wordt dan vooraf gecommuniceerd. De camera's worden dan uitgezet, zodat leerlingen niet zichtbaar in beeld zijn.
- Voor opnames dient van te voren overeenstemming te zijn en toestemming voor zijn gegeven.