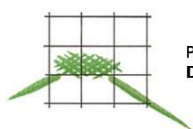


Protocol digitale media PCBO Rheden 2024-2025



P.C. Basisschool
De Arnhorst



PC Daltonschool
Prins Bernhard



Inhoud

Inleiding.....	2
Deel 1 Gedragscode digitale media voor leerlingen	3
Beleid van de school (dit onderdeel kan school aanpassen aan de eigen visie)	4
Afspraken met ouders en leerlingen	5
Afspraken met leerlingen	6
Afspraken rondom het gebruik van door kinderen meegebrachte media devices	7
Deel 2 Gedragscode digitale media voor medewerkers	9
Afspraken met medewerkers over gebruik	9
Afspraken over veilig e-mailen	11
Afspraken over privégebruik van e-mail en internet op het werk	13
Afspraken over controleren van gebruik van e-mail en internet op het werk.....	14
Afspraken over nieuwe onderwijsapps etc.	15
Afspraken over gebruik eigen devices.....	15

Inleiding

Bij PCBO Rheden vinden wij het belangrijk dat medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen op een veilige manier gebruik maken van internet, email en sociale media aan de hand van vooraf opgestelde richtlijnen. Deze zijn verwerkt in dit protocol. Het protocol bestaat uit een **gedragscode digitale media voor enerzijds leerlingen en ouders** en anderzijds **medewerkers**.

Deze tweedeling is gemaakt omdat er deels andere afspraken gelden en de toonzetting en de mogelijke gevolgen bij niet naleven van de afspraken verschillen voor beide groepen. Dit protocol wordt op de scholen waar nodig aangepast aan de eigen visie.

Het gebruik van het internet bij PCBO Rheden

De leerlingen van PCBO Rheden maken gebruik van internet. Ze maken gebruik van zoekmachines, Windows office- programma's, Snappet, Moo en een aantal online oefenprogramma's.

Afspraken

De afspraken voor digitale media staan hieronder. Het is de bedoeling dat dit protocol in het team en met de leerlingen besproken wordt. Daarnaast moet het voor ouders te vinden zijn op de schoolwebsite.

Uitgangspunten

1. PCBO Rheden onderkent het belang van sociale media;
2. Dit protocol draagt bij aan een goed en veilig school- en onderwijsklimaat;
3. Dit protocol bevordert dat de instelling, medewerkers, leerlingen en ouders op de sociale media communiceren in het verlengde van de missie en visie van de onderwijsinstelling en daarbij de reguliere fatsoensnormen in acht nemen. Dit betekent dat we respect voor de school en elkaar hebben, dat we verdraagzaam zijn en iedereen in zijn waarde laten;
4. De gebruikers van sociale media dienen rekening te houden met de goede naam van de school en van eenieder die betrokken is bij de school;
5. Het protocol dient ervoor alle betrokkenen bij de onderwijsinstelling, te beschermen tegen de mogelijke negatieve gevolgen van de sociale media.

Doelgroep en reikwijdte

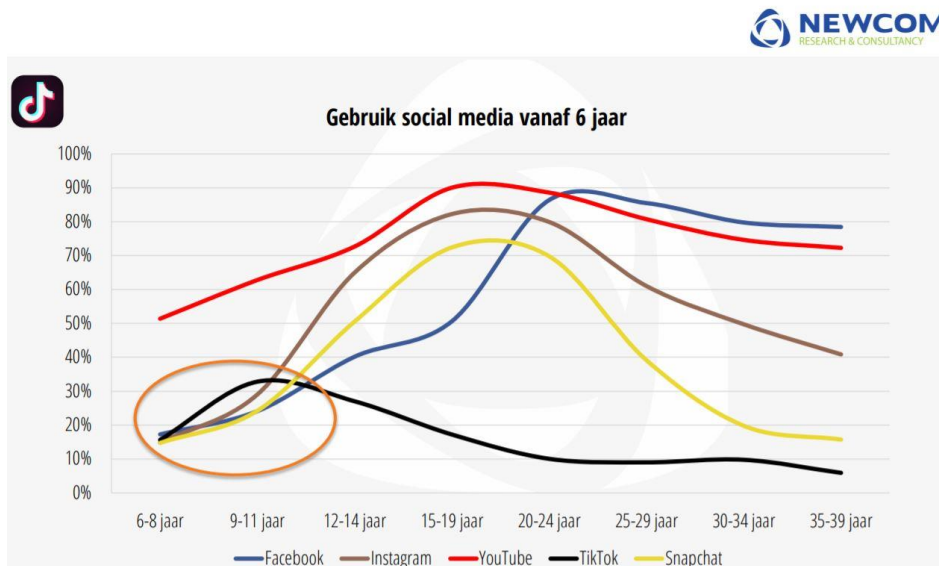
1. Deze richtlijnen zijn bedoeld voor alle betrokkenen die deel uitmaken van de schoolgemeenschap, dat wil zeggen medewerkers, leerlingen, ouders/verzorgers en mensen die op een andere manier verbonden zijn aan de scholen van PCBO Rheden.
2. De richtlijnen in dit protocol hebben betrekking op berichten die direct of indirect gerelateerd zijn aan de school of wanneer sprake is een overlap is tussen school, werk en privé.

Dit protocol is ook opgenomen in het ICT-beleidsplan en heeft instemming van de GMR nodig. Het wordt geplaatst op SharePoint, Intranet en op de websites van de scholen. Tevens wordt het protocol met ouders gecommuniceerd middels de nieuwsbrief. Het protocol moet worden besproken met leerlingen en medewerkers.

Deel 1 Gedragscode digitale media voor leerlingen

Inleiding

Sociale media spelen een belangrijke rol in het leven van leerlingen en leerkrachten. Uit het Nationale Sociale Media Onderzoek 2020 blijkt dat met name YouTube en TikTok populair zijn bij kinderen van 6 tot 12 jaar.



Het gebruik van sociale media is onderdeel van het gedrag van leerlingen binnen de school. Sociale media kunnen helpen om het onderwijs te verbeteren en de lessen leuker te maken, om contact te houden met vrienden, te experimenteren en grenzen te verleggen. Maar sociale media brengen ook risico's met zich mee, zoals pesten en het ongewild delen van foto's of andere gegevens.

Met deze gedragscode kan het gesprek op school, in de klas maar ook thuis gevoerd worden over wat er acceptabel is op sociale media (en wat niet). De afspraken gelden voor het gebruik van sociale media op mobiele telefoons en andere (mobiele) devices. Niet alleen op school en in de klas, maar ook in het mediagebruik buiten de school. Deze gedragscode is van toepassing op alle leerlingen en ouders (hieronder vallen ook verzorgers) van de scholen van PCBO Rheden, onafhankelijk van de plaats waar zij hun sociale media gebruiken.

Onder het gebruik van sociale media verstaan we het gebruik van programma's waarmee online informatie kan worden opgezocht, gedeeld en gepresenteerd. Denk bijvoorbeeld aan Facebook, Twitter, Instagram, YouTube, Snapchat maar ook alle (nieuwe) hiermee vergelijkbare programma's en apps zoals TikTok.

In gevallen waarin deze gedragscode niet voorziet, alsmede in geval van geschillen over de uitleg of de toepassing van deze gedragscode, beslist de school of het bevoegd gezag.

Het bevoegd gezag kan deze gedragscode met instemming van de oudergeleding van de GMR wijzigen of intrekken. De oudergeleding van de MR van de scholen van PCBO Rheden hebben instemmingsrecht ten aanzien van de vaststelling of wijziging van het school specifieke beleidsdeel van deze gedragscode.

Beleid van de school (dit onderdeel kan school aanpassen aan de eigen visie)

1. Internet wordt gebruikt voor educatieve doeleinden.
2. Er wordt niet gewerkt op internet, zonder dat er toestemming is van leerkrachten. Het gebruik van internet is een verantwoordelijkheid voor het hele team, medewerkers, leerlingen en ouders. We maken regelmatig looprondes en maken gebruik van schermcontrole, meekijken op de devices op afstand.
3. Leerlingen mogen met toestemming gebruik maken van spelletjessites. De begeleider is verantwoordelijk voor de inhoud van deze spellen. Geen spellen met agressie, geweld ect.
4. Er worden geen websites gebruikt die niet aan de algemeen geldende fatsoensnormen voldoen.
5. Er wordt aan de kinderen uitgelegd, waarom zij bepaalde websites wel of niet mogen gebruiken.
6. De groepsleerkracht draagt zorg voor een omgeving, waarin kinderen open kunnen vertellen wanneer zij op een ongewenste, onbedoelde site terechtkomen. Het is meestal niet bewust.
7. Informatie die terug te voeren is op leerlingen, ouders, medewerkers en vrijwilligers mag niet op het internet terechtkomen.
8. Jaarlijks krijgen de leerlingen les in mediawijsheid. Dit zijn workshops van de mediacoach van Bibliotheek Veluwezoom en van de co-teachers van Heutink-ICT.
9. De school plaatst geen beeldmateriaal van leerlingen op het internet/ sociale media, tenzij ouders hiervoor toestemming hebben gegeven.
10. Ouders kunnen met vragen en/of opmerkingen over beeldmateriaal op onze site altijd terecht bij de directie van de school.
11. Stagiaires of buitenstaanders die voor een opdracht moeten filmen of ander beeldmateriaal willen maken, vragen vooraf via de leerkracht toestemming aan ouders.

Afspraken met ouders en leerlingen

1. Iedereen is verantwoordelijk voor wat hij (of zij) zelf plaatst op sociale media en kan daarop aangesproken worden. Ook het doorsturen (forwarden) en herplaatsen (retweeten) vallen hieronder.
2. Behandel iedereen netjes en met respect en laat hem in zijn waarde.
3. Verspreid geen informatie, foto's of video's over anderen als zij daar geen toestemming voor hebben gegeven of als zij daar negatieve gevolgen van kunnen ondervinden.
4. Zet geen foto's van leerlingen of leerkrachten op internet of sociale media zonder de uitdrukkelijke toestemming van de ouders of leerkrachten.
5. Het is niet toegestaan om opnames te maken van lessen op afstand en deze te delen op sociale media.
6. Zet geen vertrouwelijke informatie over de school op sociale media.
7. Gebruik e-mail, internet en sociale media zo veilig mogelijk (beveiligde verbinding etc.).
8. Houd rekening met de goede naam van de school.
9. Ga niet in discussie met een leerling, ouder of leerkracht op sociale media.
10. We helpen elkaar om goed en verstandig met sociale media om te gaan en we spreken elkaar daarop aan.
11. Indien ouders kennis hebben van ontoelaatbare en/of grensoverschrijdende communicatie in woord, beeld en/of geluid dan dienen zij dat te melden bij de leerkracht of de schoolleiding.
12. Als er geconstateerd wordt dat de afspraken niet worden nageleefd, wordt dit eerst met de leerling en/of zijn ouders besproken. Bij een ernstige overtreding kan de directie van de school besluiten een maatregel op te leggen, die kan bestaan uit het in beslag nemen van de telefoon (of vergelijkbare communicatieapparatuur), het uitsluiten van toegang tot het netwerk, het geven van een disciplinaire maatregel (straf) of in het uiterste geval het schorsen of verwijderen van de leerling van school. Hierbij wordt er altijd contact opgenomen met de ouders van de leerling. Daarnaast kan de directie contact opnemen met de politie indien er sprake is van een strafbaar feit.

Afspraken met leerlingen

1. Je kunt gebruik maken van verschillende zoekmachines, AI en Chat GPT. Van de leerkracht leer je (kritisch) om te gaan met de zoekresultaten.
2. Geef nooit persoonlijke informatie door op internet, zoals namen, adressen en telefoonnummers, zonder toestemming van de groepsleerkracht.
3. Geef je wachtwoord NOOIT aan een ander.
4. Maak jezelf zonder toestemming nergens lid van.
5. Download zonder toestemming geen bestanden.
6. Gebruik geen USB- stick of andere gegevensdragers, maar sla je werk in de Cloud op (MOO/ OneDrive).
7. Wanneer je even wegloopt van je device, vergrendel je het scherm.
8. Als je klaar bent, log je uit en sluit je het device correct af.
9. Vertel het je groepsleerkracht meteen als je informatie tegenkomt waardoor je je niet prettig voelt of waarvan je weet dat dat niet hoort. Houd je je aan de afspraken, dan is het niet jouw schuld dat je zulke informatie tegenkomt.
10. Leg nooit verdere contacten/ spreek nooit af met iemand zonder toestemming van je groepsleerkracht.
11. Verstuur bij berichten nooit foto's van jezelf of van anderen zonder toestemming van je groepsleerkracht.
12. Beantwoord nooit berichten waarbij je je niet prettig voelt of waar dingen in staan waarvan je weet dat dat niet hoort. Het is niet jouw schuld dat je zulke berichten krijgt.
13. Verstuur ook zelf dergelijke berichten niet.
14. Spreek van tevoren met je leerkracht af wat je op internet wilt gaan doen.
15. Als je anderen op "ongewenste" pagina's ziet dan mag je dat melden. Wij vinden dat géén klikken.
16. Het is niet toegestaan om op school te hacken en ongeoorloofd toegang te krijgen tot niet-openbare websites of programma's.

Afspraken rondom het gebruik van door kinderen meegebrachte media devices

In het primair onderwijs en het (voortgezet) speciaal (basis)onderwijs zijn mobiele telefoons, tablets en smartwatches vanaf het schooljaar 2024 -2025 niet meer toegestaan op school. Dit omdat ze afleiden en ervoor zorgen dat leerlingen slechter presteren. Wij sluiten ons daarmee aan bij de afspraak die al eerder werd gemaakt met middelbare scholen.

Dit houdt in dat:

1. Alleen als de mobiele telefoons noodzakelijk zijn voor de inhoud van de les mogen ze worden gebruikt, bijvoorbeeld in een les over mediawijsheid.
2. Een telefoon is ook toegestaan wanneer leerlingen ervan afhankelijk zijn, bijvoorbeeld om medische redenen of vanwege een beperking. Indien uw kind, als uitzondering, toch een telefoon of smartwatch bij zich heeft dan moet deze uitgeschakeld in de tas blijven. De leerkracht wordt op de hoogte gesteld van deze uitzondering.
3. Indien nodig kan de telefoon van school gebruikt worden.
4. Leerlingen mogen met een mobiele telefoon of een ander mobiel device nooit foto's of filmpjes van de school, een les, de leerkracht of medeleerlingen maken en/ of doorsturen naar anderen dan wel posten op sociale media. Uiteraard hebben leerkrachten een voorbeeldfunctie ook op dit gebied. Zij gebruiken de mobiele telefoon verstandig en leggen uit waarom er een verschil is tussen leerlingen en leerkracht (denk aan Parro ouderapp e.d.).
5. De school is er niet verantwoordelijk voor wanneer er iets vermist wordt of stuk gaat. We rekenen erop dat iedereen voorzichtig omgaat met eigendommen van anderen en van de school.
6. Door de telefoon of smartwatch thuis te houden verwachten we ook dat de sociale veiligheid rond de school vergroot wordt.
7. Er is een gastennetwerk op school. Deze is beschikbaar voor schoolactiviteiten.
8. Mag de school (preventief) berichten controleren op de telefoon of een andere device van leerlingen? Mass surveillance is verboden. Alleen bij een concrete verdenking mag de school in overleg met de ouders om inzage vragen. Voorwaarde is wel dat de school dit in haar schoolreglement heeft geregeld. Als de leerling en ouders niet willen meewerken dan kan de school contact opnemen met de politie.
9. Mag de school tijdens de les meekijken op tablets, computers of telefoons van haar leerlingen? De school mag tijdens de les klassikaal controleren. Dit om te voorkomen dat leerlingen tijdens de les bijv. gaan TikTokken.
10. De school mag een leerlingdevice bevriezen, internetsites en/of apps blokkeren, geforceerd bepaalde websites aansturen, controleren of leerlingen op de juiste sites zitten, ongewenste vensters sluiten en bekijken wat er op hun scherm staat.

De school mag geen leerling-device volledig overnemen en mag ook het beeldmateriaal niet bewaren. De school mag ook de camerafunctie van de leerling besturen.

11. Bij overtreden van de regels kan het device worden ingenomen door een leerkracht/verantwoordelijke. De leerkracht/verantwoordelijke bepaalt wanneer deze weer teruggegeven wordt. De leerkracht/verantwoordelijke neemt eventueel contact op met ouders.

Bronnen

- *Model protocol sociale media van Verus (september 2020)*
- *Modelreglement internet en sociale media op school van Kennisnet*
- <https://aanpakibp.kennisnet.nl/eigen-devices-van-leerlingen/>
- *Nationale Sociale Media Onderzoek 2020*
- <https://www.apsitdiensten.nl/privacy/avg-naleven/schermen-overnemen>

Deel 2 Gedragscode digitale media voor medewerkers

Inleiding

E-mail, internet en sociale media zijn niet meer weg te denken in onze maatschappij en dus ook niet bij iedereen die betrokken is bij onderwijs. Sociale media kunnen een goede bijdrage leveren aan de professionaliteit van onderwijspersoneel en de kwaliteit van het onderwijs. Uitgangspunt is dat professionals zelf weten hoe zij hiermee verstandig omgaan. Het digitale gedrag op sociale media wijkt niet af van het real life gedrag binnen de school.

Deze gedragscode heeft als doel de dialoog over het gebruik ervan op gang te brengen en een handreiking te bieden voor meer duidelijkheid in het grijze gebied tussen binnen- en buitenschools mediagebruik. Onder het gebruik van sociale media verstaan we het gebruik van programma's waarmee online informatie kan worden opgezocht, gedeeld en gepresenteerd. Denk bijvoorbeeld aan Facebook, Twitter, Instagram, YouTube, Snapchat en LinkedIn maar ook alle (nieuwe) hiermee vergelijkbare programma's en apps.

Deze gedragscode is van toepassing op alle medewerkers van PCBO Rheden, onafhankelijk van de plaats waar zij email, internet of sociale media gebruiken.

In gevallen waarin deze gedragscode niet voorziet, alsmede in geval van geschillen over de uitleg of de toepassing van deze gedragscode, beslist het bevoegd gezag.

PCBO Rheden kan deze gedragscode met instemming van de personeelsgeleding van de GMR wijzigen of intrekken.

Afspraken met medewerkers over gebruik

1. Iedereen is verantwoordelijk voor wat hij (of zij) zelf plaatst op sociale media en kan daarop aangesproken worden. Ook het doorsturen (forwarden) en herplaatsen (retweeten) vallen hieronder.
2. Behandel iedereen netjes en met respect en laat hem in zijn waarde.
3. Verspreid geen informatie, foto's of video's over anderen als zij daar geen toestemming voor hebben gegeven of als zij daar negatieve gevolgen van kunnen ondervinden.
4. Zet geen foto's van leerlingen op internet of sociale media zonder de uitdrukkelijke toestemming van de ouders.
5. Zet geen vertrouwelijke informatie op sociale media.
6. Gebruik e-mail, internet en sociale media zo veilig mogelijk (clean desk, clear screen, beveiligde verbinding etc.).
7. Voorkom lekken van interne en vertrouwelijke informatie en meld diefstal of verlies van je smartphone, laptop etc. direct bij je schoolleiding.

8. Maak bij een onderwijsinhoudelijk onderwerp duidelijk of je dit namens je school doet of op persoonlijke titel.
9. Leidinggevend zijn altijd vertegenwoordiger van de school – ook als zij een privémening verkondigen. Bij twijfel publiceren zij niet.
10. Het is niet toegestaan standpunten en/of overtuigingen uit te dragen die in strijd zijn met de missie en visie van de school of PCBO Rheden en de uitgangspunten van deze gedragscode.
11. Houd rekening met de goede naam van de school.
12. Ga niet in discussie met een leerling, ouder of medewerker op sociale media.
13. Het is niet toegestaan om met een privé account 'vrienden' te worden met leerlingen op sociale media.
14. We helpen elkaar om goed en verstandig met sociale media om te gaan en we spreken elkaar daarop aan.
15. Indien medewerkers kennis hebben van ontoelaatbare en/of grensoverschrijdende communicatie in woord, beeld en/of geluid dan dienen zij dat te melden bij de schoolleiding of het bevoegd gezag.
16. Medewerkers die in strijd handelen met deze gedragscode maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie over dit onderwerp wordt opgenomen in het personeelsdossier. Indien de werkgever/ directeur de wijze van communiceren door een medewerker(s) als 'grensoverschrijdend' kwalificeert, dan wordt dit telefonisch gemeld bij de Landelijke Vertrouwensinspecteur (0900 – 1113111). Afhankelijk van de ernst van de uitingen en/of gedragingen van medewerkers en de gevolgen daarvan worden rechtspositionele maatregelen genomen die variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet. Wanneer uitingen of gedragingen van medewerkers mogelijk een strafrechtelijke overtreding inhouden kan door de school of het bevoegd gezag melding of aangifte bij de politie worden gedaan.

Afspraken over veilig e-mailen

Aan het verzenden van informatie via e-mail zitten risico's. Dus wil je persoonsgegevens via e-mail versturen dan ben je als organisatie verantwoordelijk voor dat je die gegevens veilig verstuurt. Hieronder staan de spelregels die we binnen PCBO Rheden hebben afgesproken. Heb je over deze richtlijn vragen dan kan je die mailen naar: bestuur@pcbo-rheden.nl.

1. Je moet een onderscheid maken tussen mailen binnen en buiten het netwerk van PCBO Rheden. Het netwerk van PCBO Rheden bestaat uit alle e-mailadressen die eindigen op @pcbo-rheden.nl. Binnen dit netwerk worden alle gegevens encrypted verstuurd. Mailen naar een ander @pcbo-rheden.nl is dan ook qua verbinding veilig.
2. Soms komt het voor dat iemand van de school gebruik maakt van jouw computer of laptop. Wil je ook de inhoud van je mail beveiligen dan moet je een wachtwoord gebruiken:
 - Klik in een bericht dat je opstelt in het bovenmenu op het tabblad Opties.
 - Klik in het vervolgmenu op **Machtigingen(slotje)** en selecteer **versleutelen**.
 - Stel je bericht op en klik op **Verzenden**.
3. Buiten het netwerk van PCBO Rheden moet je onderscheid maken tussen ouders en professionele organisaties zoals het SWV PassendWijs, GGD of gemeente.
4. Bestanden met gevoelige of vertrouwelijke informatie naar professionele organisaties moet je met een wachtwoord beveiligen tenzij de organisatie gebruik maakt van een beveiligde applicatie bv. Kindkans van Passendwijs. Hieronder bij 7 vind je een instructie hoe je een bestand met een wachtwoord beveiligt. Het wachtwoord van het beveiligde bestand stuur je in een aparte e-mail of sms naar je contactpersoon van die organisatie.
5. Moet je ouders bepaalde gevoelige of vertrouwelijke informatie over hun kind meegeven bijv. voor een logopedist of psycholoog (en kan dat niet via een beveiligde applicatie worden verstuurd) dan vraag je de ouders hoe zij die informatie willen ontvangen. Ouders kunnen kiezen uit 3 uitmogelijkheden:
 - E-mail (zonder wachtwoord)
 - Post
 - In een gesloten enveloppe op school aan de ouders

Je legt de keuze van de ouders schriftelijk vast in het leerlingendossier.

6. E-mail is bedoeld voor communicatie en niet voor archief. Privacygevoelige documenten zoals verslagen, observaties etc. moeten geplaatst worden in een daarvoor bestemde en beveiligde omgeving, een LAS (ParnasSys)
7. Hoe beveilig ik een bestand met een wachtwoord?

Een wachtwoord toevoegen aan een PDF-bestand

Binnen PCBO Rheden wordt geen gebruik gemaakt van een betaalde Acrobat Pro variant. Hierdoor is het niet mogelijk om een Pdf-bestand direct te beveiligen met een wachtwoord. Het toevoegen en verwijderen van wachtwoorden aan een pdf-bestand is hierdoor iets omslachtiger. Het toevoegen werkt alleen wanneer je een Word document opslaat als PDF, tijdens dit proces kun je een wachtwoord toevoegen.

- Open het Word document
- Klik op Bestand -> Opslaan als -> Bladeren
- Geef het bestand een naam en kies bij *opslaan als* voor PDF(*.pdf)
- Klik op **Meer opties** en dan op **Opties** en zet een vinkje bij: '**het document met een wachtwoord versleutelen**' en dan **OK**.
- Geef hierna 2x het wachtwoord op.
- Nu is het Word document opgeslagen als een beveiligd PDF-bestand.

Een wachtwoord verwijderen van een PDF-bestand

Binnen Adobe Acrobat Pro is dit zo te regelen maar dit pakket gebruiken we niet. Je doet daarom het volgende. Wanneer je het geopende bestand afdrukt op een PDF-printer wordt het weer een onbeveiligde PDF.

In **Windows 10** is al een PDF-printer geïnstalleerd. In het kort:

- Het beveiligde Pdf-bestand openen
- Klik op Bestand -> Afdrukken
- Selecteer bij printers **Microsoft print tot PDF** en klik op Print
- Selecteer nu de locatie en geef een bestandsnaam op.
- Nu heb je weer een onbeveiligd Pdf-bestand.

In **Windows 11** is al een PDF-printer geïnstalleerd. In het kort:

- Het beveiligde Pdf-bestand openen
- Klik op **Afdrukken**
- Selecteer bij printers **Microsoft print tot PDF** en klik op **Print**
- Selecteer nu de locatie en geef een bestandsnaam op.
- Nu heb je weer een onbeveiligd Pdf-bestand.

Een wachtwoord toevoegen aan een Word-bestand

- Klik op het menu **Bestand -> Info ->** en op de knop **Document beveiligen**.
- Klik op **Versleutelen met wachtwoord**.
- Typ een wachtwoord en klik op **OK**, typ nogmaals uw wachtwoord en klik op **OK**.
- Het **document** is nu beveiligd.

Het wachtwoord verwijderen van een Word-document

- Open het document, voer zo nodig het wachtwoord in.
- Klik op **Bestand -> Info -> Document beveiligen**.
- Klik op **Versleutelen met wachtwoord**.
- Wis (met Backspace of Del) het wachtwoord en klik op **OK**.

Wachtwoordtips

Hoe sterker je wachtwoord hoe kleiner de kans dat het gekraakt kan worden. Hieronder een aantal tips voor een sterk wachtwoord.

- **Hoe meer tekens, des te veiliger.** 8 tekens is aan de korte kant. Een wachtwoord met 12 tekens of meer is veel sterker. Een wachtwoord van 12 in plaats van 8 tekens maakt het wachtwoord tot 80 miljoen keer zo sterk.
- **Cijfers, hoofdletters en speciale tekens** (&? #! %, enz.) versterken het wachtwoord.
- Gebruik **een wachtzin**, die onthoud je makkelijker. Voorbeeld: IkHeb100Fietspompen.
- Gebruik wachzzinnen van **minimaal 4 woorden**. Gebruik geen spreekwoord of bekende zin, maar het hoeft niet heel ingewikkeld te zijn. Een ander voorbeeld is 131KilometerIsTeSnel. Helaas werken te lange wachtwoordzinnen niet altijd. Veel websites hebben een maximale wachtwoordlengte die tussen de 10 en 20 tekens ligt.
- Het wachtwoord mag geen makkelijk te raden **persoonlijke informatie** bevatten, zoals een naam, geboortedatum of adres.
- Gebruik **verschillende wachtwoorden** voor elke website en dienst.
- Pas wachtwoorden aan als het programma het aangeeft. Of pas wachtwoorden minimaal 1 keer per jaar aan. Niet te vaak, want je moet het wel kunnen onthouden.
- Je kunt een lijstje wachtwoorden bijhouden in een **beveiligd** Word-document of in een bestandje op je telefoon. Wachtwoorden kan je ook opslaan in een wachtwoordenmanager. Gebruik hierbij een tweestapsverificatie(MFA).

Afspraken over privégebruik van e-mail en internet op het werk

1. Uitgangspunt is dat medewerkers hun school e-mail en school internet gebruiken voor het werk.
2. Medewerkers mogen hun school e-mail en school internet op het werk ook privé gebruiken op voorwaarde dat dit qua tijd beperkt is, niet storend is voor hun dagelijkse werkzaamheden en geen verboden handelingen oplevert.
3. Let op: synchroniseert een medewerker de school e-mail met zijn eigen device (smartphone, tablet etc.) dan kan PCBO Rheden bij verlies of diefstal van het device gebruikmaken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het device gewist worden.
4. Medewerkers mogen hun school e-mail niet gebruiken voor het verzenden van berichten:
 - Met een pornografische, racistische, discriminerende, beledigende en/of aanstootgevende inhoud;
 - Met een (seksueel) intimiderende inhoud;
 - Die (kunnen) aanzetten tot haat en/of geweld.
5. Medewerkers mogen op school internet geen websites bezoeken die pornografisch, racistisch, discriminerend, beledigend en/of aanstootgevend materiaal bevatten. Ook mogen zij dergelijk materiaal niet downloaden.

6. Medewerkers mogen op school internet geen films, muziek, software etc. downloaden van een illegale bron.
7. Medewerkers mogen op school internet niet deelnemen aan kansspelen.
8. Medewerkers mogen op school internet geen toegang verschaffen tot niet openbare bronnen.
9. Het is niet toegestaan om op school te hacken en ongeoorloofd toegang te krijgen tot niet-openbare websites of programma's;

Afspraken over controleren van gebruik van e-mail en internet op het werk

PCBO Rheden mag het gebruik van e-mail en internet op het werk controleren. Zij moet zich hierbij wel houden aan de voorwaarden die de AVG stelt. De belangrijkste voorwaarden zijn:

- PCBO Rheden heeft een legitiem doel (gerechtvaardigd belang) bij het controleren en dat weegt zwaarder dan het privacybelang van zijn medewerkers. Van het doel van de controle hangt af hoe omvangrijk de controle mag zijn.
- De controle moet noodzakelijk zijn, dat wil zeggen er is geen andere manier mogelijk om dit doel te bereiken die minder ingrijpend is voor de privacy van zijn medewerkers.
- PCBO Rheden informeert haar medewerkers wat toegestaan en wat verboden is, dat controle mogelijk is en op welke manier dat gebeurt.

Met welk doel controleert de school of het bevoegd gezag het gebruik van e-mail en internet?

- Testen van de systeem- en netwerkbeveiliging;
- Voorkomen van seksuele intimidatie, discriminatie etc.;
- Voorkomen van negatieve publiciteit;
- Tegengaan van onnodig beslag op systeem- en/of netwerkcapaciteit etc.

Welke voorwaarden gelden voor controle?

- PCBO Rheden controleert het gebruik van e-mail en internet op het werk alleen in het kader van de handhaving van de doelen van deze gedragscode (zie art. 2).
- In beginsel vindt controle plaats op het niveau van getotaliseerde gegevens die niet individueel herleidbaar zijn.
- Bij vermoeden van ongeoorloofd gebruik is tijdelijk gerichte controle mogelijk. In beginsel beperkt controle zich tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen kan controle op inhoud plaatsvinden.
- Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
Bij ongeoorloofd gebruik vindt altijd een gesprek met de betrokken medewerker plaats. Hierbij wordt de medewerker op de consequenties gewezen wanneer hij of zij niet stopt met het ongeoorloofd gebruik. Op verzoek van de medewerker verschaft PCBO Rheden inzage in de gegevens over het eigen gebruik.
- In principe controleert PCBO Rheden geen e-mails van leden van de (G)MR onderling, van vertrouwenspersonen, van bedrijfsartsen en van eenieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen. Dit geldt niet voor de veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van worden afgeweken.

- Gegevens over e-mail- en internetgebruik worden niet langer bewaard dan noodzakelijk met een bewaartermijn van ten hoogste 6 maanden.

Wat zijn de rechten van medewerkers?

- PCBO Rheden informeert iedere (nieuwe) medewerker over de inhoud en strekking van deze gedragscode.
- Een medewerker kan PCBO Rheden verzoeken om zijn persoonsgegevens in te zien. Dat geldt ook voor de gegevens over het eigen gebruik van school e-mail en school internet.
- Hij of zij kan PCBO Rheden tevens verzoeken om zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn of in strijd met een wettelijk voorschrift zijn. Het verzoek wordt binnen 4 weken beantwoord.

Afspraken over nieuwe onderwijsapps etc.

- Nieuwe software etc. mag alleen geïnstalleerd worden na overleg met de schoolleiding en door de ICT-coördinator van de school of de bovenschoolse ICT-coördinator/ externe systeembeheerder.
- Installeren van software etc. is alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen.

Afspraken over gebruik eigen devices

Medewerkers mogen, waar nodig, op eigen devices werken, mits zij er zorgvuldig mee omgaan, virus software up to date hebben en privacygevoelige informatie opslaan in de Cloud. Dit betekent dat evt. downloads direct van de devices worden verwijderd. Daarnaast is het niet toegestaan een USB-stick of harde schijven te gebruiken. Aangezien wij de medewerkers niet hebben voorzien van een device voor thuis voeren wij op de eigen devices van medewerkers geen remote swipe uit. De medewerkers die wel een device van PCBO hebben ontvangen weten dat bij diefstal een remote swipe uitgevoerd kan worden.

We overwegen het aanschaffen van smartphones voor elke groep naar behoefte. Deze behoefte wordt per school door de directie bekeken. Dit zou kunnen gaan om 45 telefoons zonder abonnement, maar wel met een directe verbinding met de office Cloud. Hierdoor kunnen bv. gemaakte foto's van de klas direct worden opgeslagen in de Cloud. Tevens kan op deze telefoons dan een remote swipe worden uitgevoerd bij diefstal. De telefoon blijven in het betreffende klaslokaal. Het bestuur is verantwoordelijk voor datalekken.

*Remote swipe= Op afstand wissen is een beveiligingsfunctie waarmee een netwerkbeheerder of apparaat eigenaar een opdracht kan verzenden waarmee gegevens naar een computerapparaat worden verwijderd. Het wordt voornamelijk gebruikt om gegevens te wissen op een apparaat dat verloren of gestolen is, zodat de gegevens niet in gevaar komen als het apparaat in verkeerde handen valt. Het wordt ook gebruikt om gegevens te verwijderen van een apparaat dat van eigenaar of beheerder is veranderd en niet fysiek toegankelijk is om gegevens te verwijderen.

Responsible disclosure

Bij PCBO Rheden vinden wij de veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Als jij een zwakke plek in één van onze systemen hebt gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met jou samenwerken om de leerlingen, medewerkers en onze systemen beter te kunnen beschermen.

Wij vragen jou:

- Je bevindingen te mailen naar je directeur.
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer informatie te downloaden dan nodig is om het lek aan te tonen of informatie van leerlingen, leerkrachten of andere medewerkers in te kijken, te verwijderen of aan te passen;
- De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle informatie die verkregen is via het lek direct na het verhelpen van het lek te wissen;
- Geen gebruik te maken van aanvallen op de beveiliging van de school;
- De school voldoende informatie te geven om het probleem te kunnen vinden zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij meer ingewikkelde kwetsbaarheden kan extra informatie nodig zijn.

Wij beloven dat:

- Je binnen 3 dagen van ons te horen krijgt hoe we de kwetsbaarheid gaan oppakken en wanneer wij hiervoor een oplossing verwachten te hebben;
- Als je de kwetsbaarheid netjes gemeld hebt en via de bovenstaande stappen gehandeld hebt, zullen wij geen melding maken bij de politie*;
- Wij jouw melding vertrouwelijk behandelen en dat we jouw persoonlijke gegevens niet zonder jouw toestemming met anderen delen tenzij dit wettelijke verplicht is;
- Wij je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid.

** Let op: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Er bestaat een kans dat je tijdens jouw 'zoektocht' handelingen uitvoert die strafbaar zijn. Het feit dat PCBO Rheden geen aangifte tegen je zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar jouw handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.*