STICHTING
Openbaar Onderwijs
WIJK BIJ DUURSTEDE

Waar kinderen belangrijk zijn!

Handboek

Informatiebeveiliging en Privacy

INHOUD

1 Inleiding

Informatie en ICT zijn noodzakelijk in de ondersteuning van het onderwijs. Omdat we met persoonsgegevens (van onszelf, leerlingen en anderen) werken, is privacywetgeving daarop van toepassing. Deze wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen genomen moeten worden om de persoonsgegevens te beschermen.

Dit handboek is bedoeld als informatiebron voor alle medewerkers van Stichting Openbaar Onderwijs Wijk bij Duurstede. Hierin staan de afspraken die we met elkaar gemaakt hebben over informatiebeveiliging en privacy. Niet alleen vanuit de wetgeving, maar ook op basis van de normen en waarden, die wij vanuit onze visie op onderwijs met elkaar delen en uitdragen.

Met dit document wordt voldaan aan de wettelijke informatieplicht conform **Algemene Verordening Gegevensbescherming** (AVG) die in 2018 is ingegaan.

Dit document wordt vierjaarlijks herzien, of eerder indien de wetgeving wordt aangepast.

2 Algemeen

Privacy is een lastig en vaag begrip. Privacy op school gaat over de bescherming van gegevens over leerlingen, hun ouders en medewerkers. Dit wordt geregeld in de Wet bescherming persoonsgegevens. Hieronder worden vijf belangrijke uitgangspunten voor het verantwoord omgaan met persoonsgegevens samengevat (bron: Kennisnet).
Binnen Stichting Openbaar Onderwijs Wijk bij Duurstede spreken we met elkaar af dat we altijd checken of we aan deze vuistregels voldoen bij het verzamelen en verstrekken van persoonsgegevens.

Denk bij het registeren, verzamelen en verwerken van gegevens altijd aan de 5 vuistregels:	
☐	**1. Doel en doelbinding** Heb ik vooraf een doel voor de verwerking van persoonsgegevens vastgesteld? Worden de persoonsgegevens alleen gebruikt voor dat doel dat ik vooraf heb vastgelegd?
☐	**2. Grondslag** Is er minimaal een wettelijke grondslag voor de verwerking? Er is een wettelijke grondslag als… • er een wettelijke plicht bestaat om deze gegevens te verstrekken. Bijv. voor bekostiging, inspectie, overdrachtsdossier, etc.; • er toestemming is verkregen van de ouders/verzorgers. Bijv. voor de begeleiding van een leerling door externe onderwijsspecialisten, foto's op website, etc.; • de partij een publiekrechtelijke taak heeft. Bijv. de uitwisseling van informatieve gegevens met samenwerkingsverbanden; • dit nodig is voor het uitvoeren van een overeenkomst met de ouders/verzorgers. Bijv. voor de tussen schoolse opvang van kinderen; • er sprake is van een gerechtvaardigd belang, zoals het goed laten werken van digitale leermiddelen. Bijv. voor Basispoort en educatieve uitgeverijen.
☐	**3. Dataminimalisatie** Gebruik ik alleen die gegevens die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? Kan ik met minder of bijvoorbeeld anonieme gegevens werken? Bewaar ik de gegevens niet langer dan nodig?
☐	**4. Transparantie** Heb ik de leerling of zijn ouders of mijn medewerkers vooraf helder geïnformeerd over het doel van de gegevensverwerking? Heb ik uitgelegd welke gegevens worden gebruikt en met wie deze worden gedeeld?
☐	**5. Data-integriteit** Kloppen de persoonsgegevens die ik gebruik nog steeds? Zijn de gegevens op het juiste moment, op de juiste plaats en voor de juiste mensen beschikbaar? Heb ik onjuiste gegevens gecorrigeerd of verwijderd?

3 Privacy protocol

Het Privacy protocol is een document waarin nauwkeurig en op een begrijpelijke manier beschreven is welke persoonsgegevens binnen de organisatie worden verwerkt en met welk doel.

Ook is hierin te lezen wie toegang heeft tot deze gegevens, hoe de gegevens zijn beveiligd en met wie ze uitgewisseld mogen worden.
Met het protocol voldoet het bestuur aan zijn wettelijke informatieplicht, mits deze ook actief wordt aangeboden aan de ouders[1] en medewerkers. Alle betrokkenen, zoals ouders en medewerkers, moeten daarom het Privacy protocol kunnen inzien.

Het Privacy protocol is in te zien op onze website www.obswijk.nl.
Ouders kunnen het protocol ook opvragen bij de directie van de school.

Als bijlage in het Privacy protocol is een tekst opgenomen die door alle scholen van Stichting Openbaar Onderwijs Wijk bij Duurstede gebruikt kan worden om ouders via de website en de schoolgids te informeren.

Ouders worden tijdens de aanmelding geïnformeerd over de gegevens die verzameld worden door de school en wat er met die gegevens gedaan wordt. Een korte uitleg hierover is opgenomen op het inschrijfformulier dat door alle scholen van Stichting Openbaar Onderwijs Wijk bij Duurstede gebruikt wordt. Dit inschrijfformulier is toegevoegd als bijlage aan het Privacy protocol.

4 Toestemming voor foto's/video's en online diensten

In de nieuwe privacywetgeving zijn de regels rondom het publiceren van beeldmateriaal van leerlingen aangescherpt. Ouders, maar ook medewerkers, moeten altijd toestemming geven voor het gebruik van beeldmateriaal en die toestemming moet specifiek zijn. Dat betekent dat het voor ouders en medewerkers duidelijk is voor welk gebruik van het beeldmateriaal ze toestemming geven, bijvoorbeeld voor het gebruik in de website, de schoolapp, een nieuwsbrief of de schoolgids. Ouders en medewerkers hebben de mogelijkheid deze toestemming weer in te trekken.

Uiteraard zijn er in de school ook ouders die foto's of video's maken bijvoorbeeld bij feestelijke gelegenheden. De school moet een veilige omgeving zijn voor alle kinderen (en hun ouders) en zij moeten niet het risico lopen ongewenst gefotografeerd te worden. Het is daarom binnen de scholen van Stichting Openbaar Onderwijs Wijk bij Duurstede voor ouders van belang om terughoudend te zijn in het maken van foto- of video-opnames. Je kunt dit kenbaar maken door deze afspraak op te nemen in de schoolgids en op de website.

[1] Ouders kan desgewenst ook gelezen worden als verzorgers.

Wanneer er activiteiten georganiseerd worden op een externe locatie, zoals bijvoorbeeld bij een excursie, sportdag of schoolreisje is het echter lastig om het maken van beeldopnames door ouders te verbieden. Je kunt hierover wel duidelijke afspraken maken met ouders.

Voor het gebruik van online diensten door leerlingen binnen of buiten de school moeten ouders ook toestemming verlenen. Dit betekent dat wanneer leerlingen in de klas gebruik willen maken van een eigen (privé) account voor bijvoorbeeld WhatsApp of Pinterest, ouders hier vooraf toestemming voor moeten geven.

Dit betreft alleen online diensten die ook buiten de school om in het maatschappelijk verkeer gebruikt kunnen worden, dus niet voor e-mail, digitale leeromgevingen of leermiddelen waarvoor door de school zelf een account wordt verstrekt.

Deze afspraken zijn opgenomen in het inschrijfformulier dat door alle scholen van Stichting Openbaar Onderwijs Wijk bij Duurstede gebruikt wordt. Hierop geven ouders aan of zij toestemming geven voor het gebruik van beeldmateriaal en online diensten. Ouders worden er jaarlijks aan herinnerd dat deze toestemming verlengd wordt tenzij de toestemming door ouders wordt ingetrokken. Ouders kunnen te allen tijde de toestemming intrekken.

Voor het gebruik van cameratoezicht op de scholen is in een apart hoofdstuk opgenomen. Zie hoofdstuk 13. Hierin is te lezen waarom er in bepaalde gevallen gekozen kan worden voor cameratoezicht en welke afspraken daarover zijn.

5 Verwerkersovereenkomsten

In de nieuwe privacywet is bepaald dat de school afspraken moet maken met alle leveranciers van de school die leerlinggegevens verwerken in zogenaamde Verwerkersovereenkomsten. Het gaat bijvoorbeeld om uitgevers van digitaal lesmateriaal, leveranciers van toetsen, onderwijsadviesdiensten, etc.
Het belangrijkste hierbij is dat scholen, als gegevensverantwoordelijke, de regie hebben en houden over wat er gebeurt met de persoonsgegevens. Dit mag je niet overlaten aan de leverancier (verwerker). De school beslist wat de leverancier wél en niet met de gegevens mag doen.

Een uitzondering hierop is de uitwisseling van gegevens met het samenwerkingsverband in het kader van passend onderwijs. Het samenwerkingsverband is een zelfstandige organisatie die zelf verantwoordelijk is voor de gegevens van leerlingen. De wet regelt dat een school gegevens uitwisselt met het samenwerkingsverband. Hiervoor hoeft daarom geen verwerkersovereenkomst afgesloten te worden. Het blijft natuurlijk wel belangrijk om de gegevens op de juiste manier uit te wisselen.

De verwerkersovereenkomsten worden waar mogelijk bovenschools afgesloten. Hiervoor is een inventarisatie gedaan van de lopende contracten van de scholen binnen Stichting Openbaar Onderwijs Wijk bij Duurstede. Wanneer een school een contract afsluit met een nieuwe leverancier zal er een nieuwe verwerkersovereenkomst gesloten moeten worden. De school is verplicht om nieuwe contracten door te geven aan het bestuur. Wanneer het gaat om een leverancier die alleen een contract heeft met een individuele school, is de school zelf verantwoordelijk voor het afsluiten van de verwerkersovereenkomst.

Wanneer het een contract met meerdere scholen betreft wordt dit bovenschools geregeld. Voor het afsluiten van verwerkersovereenkomsten wordt gebruik gemaakt van de meest actuele model verwerkersovereenkomst, die te vinden is via https://www.privacyconvenant.nl

Binnen de stichting is een overzicht beschikbaar van de leveranciers waar de scholen op dit moment een verwerkersovereenkomst mee hebben en welke gegevens per leverancier worden verwerkt.

6 Procedure datalekken

Als er persoonsgegevens beschadigd of verloren zijn, dan moet er binnen 3 werkdagen een melding gedaan worden bij de Autoriteit Persoonsgegevens in het kader van meldplicht datalekken.

We spreken van een datalek wanneer er mogelijk persoonsgegevens (van leerlingen, hun ouders of medewerkers) in handen kunnen vallen van derden die geen toegang tot die gegevens zouden mogen hebben of wanneer er persoonsgegevens onbedoeld verloren zijn gegaan.

Voorbeelden van datalekken zijn:

- een e-mail die aan een verkeerd persoon geadresseerd is
- een kwijtgeraakte USB-stick
- inloggegevens die openbaar zijn geworden
- een gestolen iPad
- een gehackte computer

Het bevoegd gezag van de stichting is verantwoordelijk voor de bescherming van persoonsgegevens van leerlingen en personeel en moet bepalen of er een melding gedaan moet worden bij de Autoriteit Persoonsgegevens. Wanneer er een datalek ten onrechte niet wordt gemeld, kan een hoge boete opgelegd worden.

Zijn er leerlinggegevens verloren gegaan? Is je laptop gestolen? Heb je last van een virus waardoor je niet meer bij je bestanden kunt? Of vertrouw je iets niet? Dan ben je verplicht dit zo snel mogelijk te melden. Ben je dus (een device met) persoonsgegevens kwijtgeraakt of heb je onrechtmatigheden geconstateerd met betrekking tot de toegang tot persoonsgegevens? Meld dit dan direct via ICTbeheer@obswijk.nl en bij je leidinggevende.

In het Datalekken protocol is de volledige procedure melden datalekken opgenomen.

7 Toegangsbeleid

Niet alle medewerkers hebben toegang nodig tot leerlinggegevens. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien of wijzigen.

De directeur van de school is verantwoordelijk voor het verstrekken van de juiste toegang (lees: accounts met de juiste rollen en rechten). De directeur ziet er ook op toe dat de accounts worden ingetrokken na het beëindigen van een arbeids- of samenwerkingscontract of het wijzigen van functies. Daarnaast worden de accounts van systemen met persoonsgegevens periodiek gecontroleerd.

Gegevens van leerlingen met betrekking tot administratie, inschrijving, onderwijsbegeleiding en zorg worden in ParnasSys opgeslagen. De afspraken met betrekking tot de toegang tot en het verwerken van leerlinggegevens in ParnasSys zijn hieronder beschreven.

- Inloggegevens van ParnasSys worden via het e-mailadres van Stichting Openbaar Onderwijs Wijk bij Duurstede verstrekt aan de medewerker en nooit gedeeld met anderen.
- Inloggegevens worden jaarlijks vernieuwd. De gebruiker ontvangt een geautomatiseerd bericht met het verzoek om het wachtwoord te veranderen.
- Computers waar ParnasSys in de internetbrowser is geopend, worden niet onbeheerd achtergelaten.
- De optie “automatisch wachtwoord onthouden” in de internetbrowser wordt niet aangezet voor ParnasSys.

Tabel A: Toegangsrechten in ParnasSys voor medewerkers van Stichting Openbaar Onderwijs Wijk bij Duurstede

Functies/rollen	**Rol in parnassys**[1]	**Werkzaamheden**	**Niveau van toegang**[2]**:**
Bovenschools			
Bestuurder	Monitororganisatie beheerder	Sturing en beleid	Stichting
Staf	Monitororganisatie beheerder	Sturing en beleid	Stichting
School			
Leerkrachten	Leerkracht	Verzorgen onderwijs	School
Invalleerkracht	Leerkracht beperkt	Verzorgen onderwijs	Groep
Lio-stagiaire	Leerkracht beperkt	Verzorgen onderwijs	Groep
Directeur	Applicatiebeheerder	Sturing en beleid	School
Intern begeleider	Intern begeleider	Leerlingzorg	School
Administratief medewerker	Administratie / leerkracht	Administratieve taken	School

[1] Zie bijlage 3 voor toegangsrechten die standaard per rol zijn ingesteld in ParnasSys
[2] De volgende toegangsniveaus worden onderscheiden:
- Alle leerlingen in een specifieke **groep**
- Alle leerlingen per **school** of op **meerdere scholen**
- Alle leerlingen binnen de **stichting**

8 Afspraken over mobiele devices in bruikleen

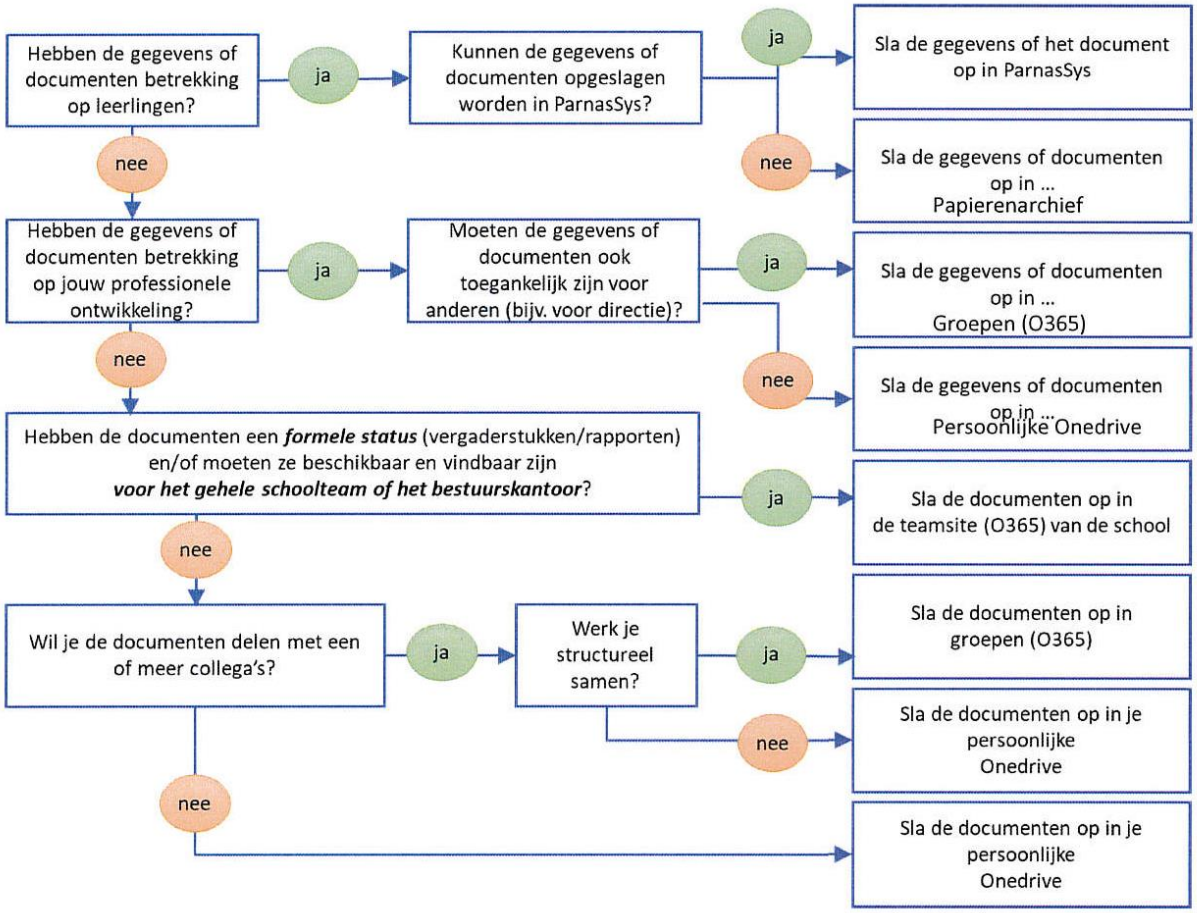
De school leent afhankelijk van de functie of aard van de werkzaamheden mobiele devices uit aan haar medewerkers. Dit kan gaan om een smartphone, tablet of een laptop. De devices zijn voorzien van beveiliging, zodat gegevens goed beschermd zijn. De devices zijn naast anti-virus o.a. voorzien van back-up functionaliteit, encryptie en worden na inname weer opgeschoond.

Aanvullend hierop wil de school nog een aantal afspraken schriftelijk vastleggen over het gebruik van het device. Deze afspraken zijn vastgelegd in bijlage 5 van dit handboek.

9 Documentmanagement

Om ervoor te zorgen dat we binnen de school onze documenten en gegevens overzichtelijk en veilig opgeslagen hebben, zijn er afspraken over wat we waar bewaren. Op deze manier zijn documenten eenvoudiger terug te vinden, maar kunnen ze ook beter afgeschermd en geback-upt worden.

In het schema hieronder kun je aan de hand van een aantal vragen bepalen op welke plek je digitale gegevens op moet slaan.



10 Archivering: vernietiging- of bewaartermijnen

Op dit moment wordt er door Kennisnet in samenspraak met het ministerie van OC&W gekeken naar bewaartermijnen van persoonsgegevens. Naar verwachting zal daar binnenkort meer duidelijk over worden. Zolang hier nog geen duidelijkheid over is houdt Stichting Openbaar Onderwijs Wijk bij Duurstede vast aan de bewaartermijnen voor leerlinggegevens zoals hieronder aangegeven, tenzij de wet anders voorschrijft.

Document/gegevens	*Verplichte bewaartermijn*	*Vastgelegd in*
Gegevens over verzuim en afwezigheid	Maximaal 5 jaar nadat leerling is uitgeschreven	Bekostigingsbesluit WPO
Gegevens in- en uitschrijving (noodzakelijk voor berekening van bekostiging)	Maximaal 5 jaar nadat leerling is uitgeschreven	Artikel 9 Bekostigingsbesluit WPO
Overige gegevens leerlingendossier, waaronder: • Verwerkingen van persoonsgegevens ter uitvoering van de **Leerplichtwet** • Verwerkingen van beoefenaren van individuele beroepen in de gezondheidszorg	Maximaal 5 jaar nadat leerling is uitgeschreven	Vrijstellingsbesluit WBP
Indien sprake is van een **bezwaar-, klachten- of gerechtelijke procedure**, dienen de persoonsgegevens **uiterlijk vijf jaar** te worden verwijderd nadat de desbetreffende leerling is uitgeschreven.	Maximaal 5 jaar nadat leerling is uitgeschreven	Vrijstellingsbesluit WBP

11 Gedragscode

Voor een veilig schoolklimaat is het belangrijk dat de afspraken rondom informatiebeveiliging en privacy door alle werknemers worden nageleefd en uitgedragen. Daarom is er een gedragscode opgesteld waaraan alle medewerkers van Stichting Openbaar Onderwijs Wijk bij Duurstede zich dienen te houden.

De afspraken zijn verdeeld in drie onderdelen:
A. Waar en hoe bewaar ik leerlinggegevens?
B. Hoe en wat communiceer ik online via e-mail en sociale media?
C. Hoe houd ik indringers op afstand?

Hieronder volgen per onderdeel de afspraken.

A. Leerlinggegevens

1. **Verwerk leerlinggegevens zoveel mogelijk digitaal.**
   Leerlinggegevens worden zoveel mogelijk digitaal opgeslagen, geraadpleegd en bewerkt in ParnasSys. Dit geldt ook voor gegevens die via ouders/verzorgers en/of externen worden ontvangen. Bewaar geen gegevens op een USB-stick.
   Gegevens die op papier aangeleverd worden, worden gescand en aan ParnasSys toegevoegd. Vergeet niet om de scan van je eigen computer te verwijderen.

2. **Formuleer gegevens die je vastlegt over een persoon zorgvuldig en professioneel.** Ouders hebben het recht om het dossier in te zien. Zorg ervoor dat de gegevens zodanig zijn geformuleerd dat dit kan. Het past ook bij je houding als onderwijsprofessional.

3. **Gebruik voor de verwerking van leerlinggegevens het netwerk van school.**
   Moet je leerlinggegevens downloaden en bewerken op een computer? Doe dit alleen op een beveiligde computer (die voorzien is van encryptie), bij voorkeur op een computer van school. Verwijder de bestanden na gebruik van je eigen computer. Zorg ervoor dat anderen (bijv. familieleden) niet bij jouw werkbestanden kunnen komen.

4. **Ga na welke afspraken er binnen de school gemaakt zijn voordat je gegevens uitwisselt met derden.**
   Wanneer je gegevens uit wilt wisselen met externen, zoals bijvoorbeeld de logopedist, een arts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en houdt daarbij ook rekening met de verdeling van het ouderlijk gezag. Voor de uitwisseling van gegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Hiervoor kun je terecht bij je IB-er of de directeur.

5. **Informeer derden (ouders, hupverleners etc.) wanneer je door hen aangeleverde informatie (zowel geschreven als mondeling) opslaat in het leerlingdossier.**
   Wanneer je bijvoorbeeld telefonisch contact hebt over een leerling met een hulpverlener en je wilt die informatie opslaan in het leerlingdossier. Informeer dan zowel de hulpverlener als de ouders welke informatie je aan het dossier toevoegt.

B. Hoe en wat communiceer ik online?

1. **Maak gebruik van een link naar ParnasSys om leerlinggegevens uit te wisselen met collega's.**
   Verstuur leerlinggegevens liever niet per mail, maar verstuur een link met de vindplaats van de benodigde gegevens in ParnasSys.

2. **Vraag ouders om toestemming om een (privé)account aan te maken voor online diensten.**
   Leerlingen moeten toestemming hebben van hun ouders/verzorgers om een (privé)account aan te maken voor online diensten zoals Pinterest, Canva, Google etc.

3. **Deel over individuele leerlingen nooit informatie via social media.**
   Doe dit vooral in persoon of desnoods via de telefoon. Wat je communiceert via social media kan makkelijk anders worden geïnterpreteerd door de lezer als je hier niet alert op bent.

4. **Deel alleen kennis en informatie over de school als het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen en de naam van de school niet schaadt.**
   Wees voorzichtig met het online uiten van standpunten. 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 je ervan bewust dat gepubliceerde uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na het verwijderen van het bericht.
   Het is voor medewerkers van Stichting Openbaar Onderwijs Wijk bij Duurstede niet toegestaan standpunten en/of overtuigingen uit te dragen die in strijd zijn met de missie en visie van de school of de stichting.

5. **Ga voordat je foto's of video's publiceert waar leerlingen op te zien zijn na of ouders hiervoor toestemming hebben gegeven.**
   Meer informatie hierover is te vinden in hoofdstuk 2

6. **Gebruik de accounts die door de school worden beheerd als je met ouders of leerlingen wilt communiceren via e-mail of social media.**
   Formuleer je boodschap ook hier professioneel en zorgvuldig, in correcte taal.

7. **Wordt geen vrienden met ouders op sociale media met je privé-account.**

8. **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.

9. **Stuur nooit een e-mailbericht door naar derden zonder de degene van wie je het bericht ontvangen hebt hierover te informeren.**

10. **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 hem bedoeld hebt. Het is dan fijn als er iemand met je meeleest voordat je hem verstuurt.

C. Hoe houd ik indringers op afstand?

11. **Zorg er bij vertrouwelijke (telefonische) gesprekken voor dat er niet kan worden meegeluisterd.**
    Trek je je even terug als een gesprek een vertrouwelijk karakter heeft of krijgt.

12. **Bewaar laptops of tablets altijd op een veilige plek, zeker tijdens vakantieperiodes.**
    Het is een open deur, maar toch gebeurt het heel erg makkelijk. Maak elkaar er dus op attent als je een laptop of tablet onbeheerd ziet liggen. Als je computer gestolen wordt, heeft dat gevolgen voor de school en de leerlingen.

13. **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 (phising)mails. In het criminele circuit is dit een veelgebruikte methode om aan jouw gegevens te komen. Ook kunnen de gegevens op je computer versleuteld worden (ransomeware).

14. **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 makkelijk afmelden. Maak er een gewoonte van om papieren op je bureau om te draaien. Zo voorkom je dat anderen informatie zien die niet voor hen is bedoeld.

15. **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 en niet voor hun ogen bestemd zijn.

16. **Laat je wachtwoorden van het leerling administratiesysteem of andere systemen met persoonsgegevens niet onthouden door je internetbrowser. En 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. Kijk **hier** voor een tip om een sterk wachtwoord te kiezen die je makkelijk kunt onthouden.

17. **Hou 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 voor jou toegankelijk moet zijn. Daarnaast herkent het systeem jou door je login, zodat het kan bijhouden wie welke gegevens heeft toegevoegd of gewijzigd.

12 Beleid Sociale Media Onderwijs

Sociale Media zijn niet meer weg te denken in onze maatschappij en dus ook niet bij iedereen die betrokken is bij scholen. Sociale media kunnen een goede bijdrage leveren aan de professionaliteit van onderwijspersoneel en de kwaliteit van het onderwijs. Net zoals bij de introductie van internet en e-mail eind vorige eeuw levert het gebruik van sociale media vragen op over het gebruik van deze individuele en meestal openbare communicatiekanalen. 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. Toch zijn er in scholen verschillen in kennis en ervaringen met, en meer of minder enthousiasme over, sociale media. Dit protocol 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 sociale media verstaat OBS Wijk Twitter, Instagram, Facebook, LinkedIn, Snapchat, Vlog's en Youtube en de wat minder bekende varianten daarop.

12.1 Onderwijskundig uitgangspunt

Internet is een informatiemedium en leerlingen moeten daar mee leren omgaan. De strategie is begeleidend confronteren. Internet is een afspiegeling van de maatschappij. Kinderen moeten leren wat goed is en wat niet, wat kan en niet kan. Begeleidend confronteren is leren omgaan met internet zoals het is, zoals het zich dagelijks aan ons voordoet. Begeleiden doen we stapje voor stapje en we bespreken de ins en outs ervan. We benaderen internet zoals we ook kinderen leren omgaan met het verkeer of de televisie.

12.2 Richtlijnen gebruik sociale media medewerkers

1. Medewerkers van Stichting Openbaar Onderwijs Wijk bij Duurstede delen kennis en andere waardevolle informatie.
2. Bij onderwijs onderwerpen maken medewerkers duidelijk of zij op persoonlijke titel of namens de school publiceren.
3. Medewerkers van Stichting Openbaar Onderwijs Wijk bij Duurstede publiceren geen vertrouwelijke informatie op sociale media.
4. Ga niet in discussie met een leerling of ouder op sociale media.
5. Schoolbestuurders, schoolleiders en leidinggevenden zijn altijd vertegenwoordiger van de school – ook als zij een privémening verkondigen. Bij twijfel niet publiceren.
6. Medewerkers van Stichting Openbaar Onderwijs Wijk bij Duurstede zijn persoonlijk verantwoordelijk voor wat zij publiceren.

7. Medewerkers van Stichting Openbaar Onderwijs Wijk bij Duurstede weten dat publicaties op sociale media altijd vindbaar zijn.
8. Bij twijfel over een publicatie of over de raakvlakken met de school zoeken medewerkers contact hun leidinggevende.
9. Stichting Openbaar Onderwijs Wijk bij Duurstede zorgt ook digitaal voor een veilig klimaat en communiceert met medewerkers, leerlingen en ouders hoe zij dit doet.
10. Stichting Openbaar Onderwijs Wijk bij Duurstede legt vast welke maatregelen zij neemt bij digitale overtredingen van medewerkers, leerlingen en ouders en communiceert dit met deze doelgroepen.

12.3 Praktische voorbeelden

Kennisdeling

Via Twitter of in Linkedingroepen (bijvoorbeeld Schooljournaal of Onderwijs 2.0) kan onderwijspersoneel zich mengen in discussies over onderwijszaken. Dit kan op basis van persoonlijke ervaringen. Als een standpunt van Stichting Openbaar Onderwijs Wijk bij Duurstede of die van de school gepubliceerd wordt, vermeldt de schrijver dit.

Verantwoordelijkheid

Hoofdregel: het gedrag van leraren op, Facebook, LinkedIn, Youtube en Twitter wijkt niet af van wat in de klas of op de school gebruikelijk is.

Don'ts:
- Foto's of filmpjes van leraren op vakantie of in beschonken toestand op een feest.
- Tweets van leraren die eindigen met '…en nu wel aan je huiswerk. Laterzz XXX…
- Te populair taalgebruik en schuttingtaal.

Veiligheid

Stichting Openbaar Onderwijs Wijk bij Duurstede heeft een verantwoordelijkheid als het gaat om de veiligheid van onderwijspersoneel en leerlingen. Dat begint met duidelijke en gecommuniceerde normen en waarden en de handhaving daarvan, ook digitaal. Stichting Openbaar Onderwijs Wijk bij Duurstede vindt dat scholen zich niet moeten laten verrassen door incidenten. Zorg voor duidelijke regels over: welke mediadragers zijn in de klas en op school toegestaan? Ben je als school betrokken in het grijze gebied tussen privé en school? Wanneer schakel je ouders in, en wanneer politie? Welke sancties hanteer je bij welke overtreding? Hoe ga je om met slachtoffers en hoe met de pers?
Communiceer de regels en afspraken duidelijk met onderwijspersoneel, leerlingen en ouders.
Voorbeelden die voor onveiligheid kunnen zorgen:
- Kleineren van leraren of leerlingen via Youtube filmpjes
- Dreigtweets van leerlingen
- Digitale seksuele intimidatie of beschuldiging ervan.

12.4 Internet en sociale media op school voor leerlingen

Bestemd voor leerlingen van Stichting Openbaar Onderwijs Wijk bij Duurstede

Sociale media spelen een belangrijke rol in het leven van leerlingen en onderwijzend personeel. 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 en 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 dit reglement kan het gesprek op school, in de klas maar ook thuis gevoerd worden over wat er gewoon is op sociale media (en wat niet). De afspraken zijn van toepassing op alle leerlingen van de scholen die vallen onder Stichting Openbaar Onderwijs Wijk bij Duurstede, voor het gebruik van mobiele telefoons en sociale media op school en in de groep, maar ook in het mediagebruik buiten de school.

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

Afspraken bij het gebruik van internet en sociale media

1. Dit reglement is van toepassing op alle leerlingen van de scholen vallend onder Stichting Openbaar Onderwijs Wijk bij Duurstede, onafhankelijk van de plaats waar zij hun sociale media gebruiken.

2. We behandelen elkaar netjes en met respect, en laten iedereen in zijn waarde. Daarom pesten, kwetsen, stalken, bedreigen, en beschadigen we elkaar niet, en maken we elkaar niet zwart.

3. Iedereen is verantwoordelijk voor wat hij/zij zelf plaatst op sociale media, en kan daarop aangesproken worden. Ook het doorsturen (forwarden) en herplaatsen (retweeten) zijn handelingen waar je op aangesproken kunt worden.

4. Zorg dat je weet hoe sociale media werkt voordat je ze gebruikt, zorg dat de instellingen goed staan en je niet meer informatie deelt dan je wilt. Alles wat wordt gecommuniceerd via internet en sociale media, blijft nog lang vindbaar.

5. Bij het gebruik van internet en sociale media houden we rekening met de goede naam van Stichting Openbaar Onderwijs Wijk bij Duurstede en de school en iedereen die daarbij betrokken is zoals docenten, onderwijsondersteunend personeel en ouders.

6. We helpen elkaar om goed en verstandig met sociale media om te gaan, en we spreken elkaar daarop aan. Als dat niet lukt, dan vragen we daarvoor hulp aan onze leraar of de directeur.

7. Het meenemen van mobiele telefoon en daarmee vergelijkbare communicatieapparatuur op school is toegestaan. Een leraar kan in verband met het leerproces leerlingen toestemming geven om een mobiele telefoon mee te nemen en te gebruiken in de klas.

8. We respecteren elkaars privacy. Bij het gebruik van internet en sociale media worden er daarom geen informatie, foto's of video's verspreidt over anderen, als zij daar geen toestemming voor hebben gegeven, of als zij daar negatieve gevolgen van kunnen ondervinden.

9. Er worden geen afspraken online gemaakt.

10. Je gebruikt een goed wachtwoord. Een goed wachtwoord bestaat uit minimaal 8 karakters waarvan kleine letters, hoofdletters en cijfers. Probeer een zin te verzinnen, dit kun je makkelijker onthouden.

11. Internet en sociale media worden alleen gebruikt voor acceptabele doeleinden. Het is daarom niet toegestaan om op school:
    - Downloaden zonder toestemming, plaatjes mag wel mits deze niet racistisch of beledigend zijn of seks, geweld of andere niet gewenste afbeeldingen bevatten.
    - Sites te bezoeken informatie te downloaden en te verspreiden die pornografisch, racistisch, discriminerend, gewelddadig, beledigend of aanstootgevend zijn;
    - Geen Youtube of muziek zonder toestemming;
    - Hacken en ongeoorloofd toegang te krijgen tot niet-openbare sites of programma's;
    - Informatie, foto's of video's te delen waarvan duidelijk is dat die niet bedoeld is om verder te verspreiden, hou je wachtwoorden geheim;
    - Verzonnen berichten versturen of een fictieve naam gebruiken als afzender;
    - Iemand lastig vallen, te achtervolgen of te 'flamen'.
    - Als iemand over de voorgaande punten informatie krijgt aangeboden, wordt dat gemeld aan de leraar of de directeur.

12. Als er gebruik wordt gemaakt van het netwerk van de school, dan mag dat de kwaliteit van het (draadloze) netwerk niet in gevaar brengen of schade aan personen of instellingen veroorzaken. Het hacken, overmatig downloaden of overbelasten van het netwerk is natuurlijk verboden.

13. Leerlingen en medewerkers van de school worden niet met elkaar 'vriend' op sociale media, tenzij het gaat om een door de medewerkers gebruikt professioneel account (waar geen persoonlijke informatie over de medewerker is geplaatst).

14. Als er geconstateerd wordt dat de afspraken niet worden nageleefd, wordt dit eerst met de betrokkene 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, het uitsluiten van toegang tot het netwerk van de school, 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.

13 Cameratoezicht

In het belang van de veiligheid, de gezondheid en het welzijn van leerlingen en medewerkers kunnen scholen ervoor kiezen om camera's op te hangen. Met het cameratoezicht worden de volgende doelen nagestreefd:

- Bewaking in verband met toegang, schade door vandalisme en diefstal
- Herkenning of identificatie van personen die bij gebeurtenissen betrokken zijn geweest
- Bevorderen van het gevoel van veiligheid
- Preventief, ter voorkoming van onwenselijk gedrag
- Ondersteuning bij opsporing van strafbare feiten

13.1 Informatievoorziening

De camera's zijn zichtbaar opgehangen, er wordt in principe geen gebruik gemaakt van verborgen camera's. In bijzondere gevallen, bij vermoeden van onrechtmatig handelen van leerlingen of personeel, kan tijdelijk een verborgen camera worden geplaatst.

Bij het betreden van de school wordt gewaarschuwd dat er cameratoezicht wordt uitgevoerd.

13.2 Bewaartermijn beelden

- De camerabeelden worden maximaal 4 weken bewaard behoudens voor de beelden van de incidenten die in behandeling zijn. Indien er in de periode geen incidenten hebben plaatsgevonden of zijn gemeld bij de schoolleiding worden de beelden verwijderd.
- Bij geconstateerde incidenten worden de daaraan te relateren camerabeelden pas verwijderd nadat het incident is afgehandeld. Camerabeelden die gebruikt worden in het kader van onderzoek, waarvan aangifte is gedaan bij de politie, worden pas vernietigd na overleg met de politie. De termijn van vier weken is in deze gevallen niet van toepassing.
- Incidenten die het bewaren van beelden noodzakelijk maken, worden geregistreerd en gedocumenteerd in een logboek. Als beelden van een incident worden bekeken, wordt daarvan melding gemaakt in een logboek. Het logboek wordt beheerd door de systeembeheerder.

13.3 Bekijken van beelden

Toestemming voor het bekijken van opgeslagen en/of actuele camerabeelden kan alleen gegeven worden door de directeur of de voorzitter College van Bestuur.

13.4 Informatie aan ouders

- Ouders van een leerling die een incident meldt dat het bekijken van camerabeelden noodzakelijk maakt, worden hiervan door de schoolleiding op de hoogte gesteld.
- Indien een leerling – in het belang van het oplossen van een incident – wordt verzocht camerabeelden te bekijken, worden ouders hiervan op de hoogte gesteld. Ouders kunnen het bekijken van de beelden desgewenst bijwonen.
- Ouders van een leerling die na het bekijken van de camerabeelden als "dader" wordt geïdentificeerd, worden hiervan door de schoolleiding op de hoogte gesteld en hebben het recht de beelden binnen de bewaartermijn uit dit protocol te bekijken.
- Camerabeelden die een incident registeren, dat aangifte bij de politie noodzakelijk maakt, kunnen desgevraagd door de politie worden bekeken. Betrokken leerlingen en ouders worden hierover geïnformeerd.

14 Vaststelling en ondertekening

Door ondertekening wordt akkoord gegaan met de inhoud van dit handboek 'Informatiebeveiliging en Privacy'.

College van Bestuur

Mevrouw H.J. Sikken
Voorzitter College van Bestuur
Datum: 24 mei 2018

Namens de Gemeenschappelijke Medezeggenschapsraad

De heer G. van Rijswijk
Voorzitter Gemeenschappelijke Medezeggenschapsraad
Datum: 24 mei 2018

Bijlage 1 - Formulier Toestemming gebruik foto's, video's en adressenlijst

Toestemming gebruik foto's, video's en adressenlijst

[datum]

Beste ouder/verzorger,

Op onze school laten wij u met foto's en video's zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Bijvoorbeeld tijdens activiteiten, schoolreisjes en in de lessen. Ook uw zoon/dochter kan op deze foto's (en soms in video's) te zien zijn. Foto's kunnen getoond worden op:

- het twitteraccount (@[NAAM]),
- de website (www.[NAAM}),
- de schoolapp
- in de schoolgids en jaarkalender, (digitaal en papier)
- de afgeschermde fotopagina (adres en inlog worden via de administratie verstrekt),
- de facebookpagina, ([NAAM])

Natuurlijk gaan we zorgvuldig om met foto's en video's. Wij plaatsen geen foto's waardoor leerlingen schade kunnen ondervinden. We plaatsen bij foto's en video's geen namen van leerlingen. Op sociale media plaatsen we geen foto's van individuele kinderen, alleen kinderen in groepsverband en we maken deze foto's bij voorkeur van de zijkant of van een afstand.

We vinden het belangrijk om uw toestemming te vragen voor het gebruik van foto's en video's van uw zoon/dochter. Het is goed mogelijk dat u niet wilt dat foto's van uw kind op internet verschijnen.

Via het formulier op de achterzijde vragen wij uw toestemming voor het gebruik van beeldmateriaal van uw zoon/dochter. U kunt het ingevulde formulier afgeven bij de leerkracht.

Uw toestemming geldt alleen voor foto's en video's die door ons, of in onze opdracht worden gemaakt. Het kan voorkomen dat andere ouders foto's maken tijdens schoolactiviteiten. De school heeft daar geen invloed op, maar wij gaan ervan uit dat deze ouders ook **terughoudend** zijn bij het plaatsen van foto's en video's op internet.

Wilt u uw toestemming samen met uw zoon/dochter bespreken?
We merken dat oudere leerlingen soms zelf een keuze willen maken om foto's te gebruiken. Als u uw keuze thuis bespreekt, dan weten ze zelf waarom het gebruik van foto's en video's wel of niet mag.

Adressenlijst
Op onze school wordt er, per groep, een lijst gemaakt met de adressen van leerlingen. Deze lijst met contactgegevens is erg praktisch om te overleggen met andere ouders, als de kinderen (buiten schooltijd) willen afspreken of als er vragen zijn rondom school, overblijf, etc. Wij vragen hierbij uw toestemming om de naam van uw kind, diens adres en uw telefoonnummer te mogen delen met de andere ouders van de groep van uw zoon of dochter. Als u er bezwaar tegen heeft, wordt de naam van uw kind niet gedeeld (en moet u daar zelf voor zorgen). Deze informatie op de groepslijst mag uitsluitend gebruikt worden voor persoonlijk gebruik onderling, en dus niet voor bijvoorbeeld reclame.

Schoolfotograaf
Ook de foto's gemaakt door onze schoolfotograaf willen wij graag onder uw aandacht brengen en toestemming voor vragen. Wij vragen dan ook uw toestemming voor de klassenfoto en voor de individuele foto (eventueel met broertje(s) en of zusje(s)).
Wij kunnen klassenfoto's op onze websites en/of sociale media plaatsen.

U mag natuurlijk altijd terugkomen op de door u gegeven toestemming. Ook mag u op een later moment alsnog toestemming geven.

Met vriendelijke groet,

[NAAM]

Hierbij verklaart ondergetekende, ouder/verzorger van
uit groep

dat foto's en video's door [NAAM] gebruikt mogen worden*:

☐ in de schoolgids, nieuwsbrief, schoolbrochure, schoolapp en schoolkalender
☐ besloten fotopagina (met wachtwoord)
☐ op de website van de school
☐ in de (digitale) nieuwsbrief
☐ op sociale media accounts van de school (Twitter, Facebook)
☐ alleen binnen de school op smartboards
☐ video opname ten behoeve van onderwijskundige doeleinden (scholing en coaching docenten en leerlingen), na beoordeling worden deze opnames vernietigd

dat de adreslijst gedeeld mag worden met de andere ouders van de groep *

☐ Naam
☐ Adres
☐ Telefoonnummer

Toestemming foto's maken door schoolfotograaf*

☐ Individuele foto (of met broertje of zusje)
☐ Groepsfoto
☐ Groepsfoto plaatsen op website en/of sociale media

* aankruisen waarvoor u toestemming geeft

Ondertekende zal terughoudend zijn met het plaatsen van foto's van andere leerlingen op eigen Sociale Media.
Ondergetekende zal zoveel mogelijk alleen zijn / haar eigen kind fotograferen.

Datum:

Naam ouder/verzorger:
Handtekening ouder/verzorger:

In geval van gescheiden ouders moet dit formulier door beide ouders ondertekend worden:

Naam ouder/verzorger:
Handtekening ouder/verzorger:

U kunt op elk desgewenst moment uw toestemming intrekken. Neem hiervoor contact op met de leerkracht van uw kind(eren).

Bijlage 2 - Formulier Toestemming gebruik Sociale media

Toestemming gebruik Sociale media

[datum]

Beste ouder/verzorger,

Sociale media spelen een belangrijke rol in het leven van leerlingen en onderwijzend personeel. 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 en om contact te onderhouden met vrienden of klasgenoten. Maar sociale media brengen ook risico's met zich mee, zoals pesten en het ongewild delen van foto's of andere gegevens. Op school besteden we in ons lesprogramma hier aandacht aan. Voor het gebruik van sociale media door uw kind(eren), vragen wij uw toestemming.

U mag natuurlijk altijd terugkomen op de door u gegeven toestemming. Ook mag u op een later moment alsnog toestemming geven.

Met vriendelijke groet,

[NAAM]

Hierbij verklaart ondergetekende, ouder/verzorger van

uit groep

hij/zij onder schooltijd gebruik mag maken van sociale media* t.b.v. onderwijsdoeleinden

☐ Facebook
☐ Pinterest
☐ Whatsapp
☐ Twitter
☐ Instagram
☐

* aankruisen waarvoor u toestemming geeft

Datum:

Naam ouder/verzorger:
Handtekening ouder/verzorger:

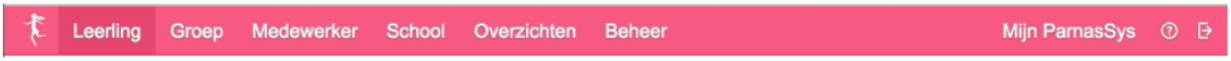
In geval van gescheiden ouders moet dit formulier door beide ouders ondertekend worden:

Naam ouder/verzorger:
Handtekening ouder/verzorger:

U kunt op elk desgewenst moment uw toestemming intrekken. Neem hiervoor contact op met de leerkracht van uw kind(eren).

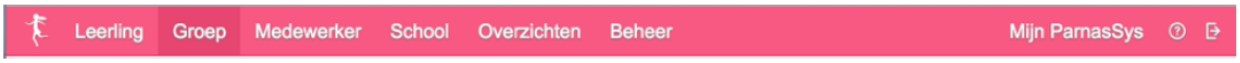
Bijlage 3 – Rollen en rechten ParnasSys

Tabblad Leerling



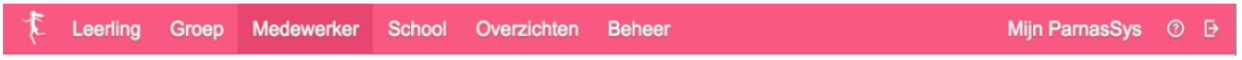
Subtab	Optie	Applicatiebeheerder	Administratie	Intern Begeleider	Leerkracht	Leerkracht beperkt	Accountbeheerder
Leerlingkaart		I	I	I	I	I	-
Personalia	Personalia	X	X	I	I	I	-
	Gezin	X	X	I	I	I	-
	Medisch	X	X	X	X	I	-
	BRON	X	X	-	-	-	-
Onderwijs	Voorgeschiedenis	X	X	X	-	-	-
	Deze school	X	X	(X)	I	I	-
	Speciaal onderwijs	X	X	X	-	-	-
	Passend onderwijs	X	X	X	-	-	-
	Vervolgonderwijs	X	X	-	-	-	-
	Absentie	X	X	X	X	-	-
	Overstapdossier klaarzetten	X	X	X	X	-	-
	Overstapdossier opvragen	X	X	-	-	-	-
Toetsen	Niet-methodetoetsen	X	-	X	X	I	-
	Methodetoetsen	X	-	X	X	I	-
	Rapporten	X	-	I	X	I	-
	Eindtoetsen	X	X	-	-	-	-
	Didactische leeftijd	X	-	X	-	-	-
	Ontwikkelprognose	X	-	X	-	-	-
	IQ-testen	X	-	X	X	-	-
Begeleiding	Plannen	X	-	X	X	I	-
	Zorgdossier	-	-	-	-	-	-
	Ontwikkelingsperspectief	X	I	X	X	I	-
	Onderwijskundig rapport	-	-	-	-	-	-
	Observatielijsten	X	-	X	X	I	-
Map	Documenten	X	-	X	(X)	(X)	-
	E-mails	X	-	X	X	X	-

Tabblad Groep



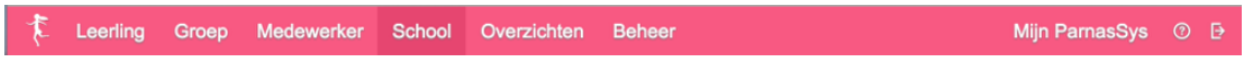
Subtab	Optie	Applicatiebeheerder	Administratie	Intern Begeleider	Leerkracht	Leerkracht beperkt	Accountbeheerder
Overzicht		I	I	I	I	I	-
Leerlingen	Jaarovergang	X	X	-	-	-	-
	Sublesgroepoverzicht	I	-	I	I	I	-
	Uitschrijven	X	X	-	-	-	-
	Plattegrond	X	X	X	X	X	-
Groepskaart		X	-	X	X	-	-
Absentie	Invoer	X	X	X	X	-	-
	Overzicht	X	X	X	X	-	-
Rooster	Lesrooster	X	X	X	X	I	-
	Leerkrachtrooster	X	X	-	X	X	-
Toetsen	Niet-methodetoetsen	X	-	X	X	I	-
	Methodetoetsen	X	-	X	X	I	-
	Rapporten	X	-	I	X	I	-
	IQ-testen	(X)	-	(X)	(X)	I	-
Begeleiding	Groepsplannen	X	-	X	X	I	-
	Plannen	X	-	X	X	I	-
	Sociogrammen	X	-	X	X	I	-
	Observatielijsten	X	-	X	X	(X)	-
Map		X	-	X	(X)	I	-

Tabblad Medewerker



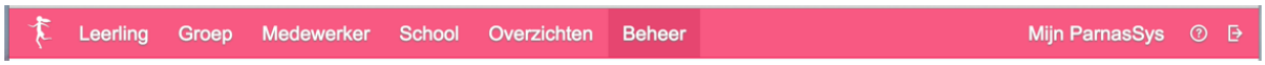
Subtab	Optie	Applicatiebeheerder	Administratie	Intern Begeleider	Leerkracht	Leerkracht beperkt	Accountbeheerder
Overzicht		I	I	I	I	I	I
Personalia	Medewerker	X	-	-	-	-	X
	Aanstelling	X	-	-	-	-	X
Map		E	E	E	E	E	E

Tabblad School



Subtab	Optie	Applicatiebeheerder	Administratie	Intern Begeleider	Leerkracht	Leerkracht beperkt	Accountbeheerder
Jaarplan	Activiteiten	X	X	I	I	I	-
	Kalender	X	X	I	I	I	-
	Urenoverzicht groepen	X	X	-	-	-	-
Import	Eindtoetsresultaten	X	X	-	-	-	-
Export	EDEX	X	X	-	-	-	-
	DOD (Digitaal Overdrachts Dossier)	X	X	-	-	-	-
Bron	Verstuur leerling BRON berichten	X	X	-	-	-	-
	Verstuur speciale BRON berichten	X	X	-	-	-	-
	Verwerk BRON terugkoppelingen	X	X	-	-	-	-
	Leerlingaantallen	X	X	-	-	-	-
OSO	Certificaat en URL	X	X	-	-	-	-
	Overstapdossiers klaarzetten	X	X	X	X	-	-
	Overstapdossiers opvragen	X	X	-	-	-	-
	Dossieraanvragen	X	X	-	-	-	-
Gespreksplanner		X	X	-	-	-	-
Map	E-mails	X	X	X	X	-	-
	Facturen	X	X	-	(X)	-	-
Controles		X	X	-	-	-	-
Info		X	X	-	-	-	-

Beheer



Subtab	Rubriek	Optie	Applicatiebeheerder	Administratie	Intern Begeleider	Leerkracht	Leerkracht beperkt	Accountbeheerder
Beheer	Algemeen	Briefhoofd	X	-	-	-	-	-
		Beperkingen	X	-	-	-	-	-
		Nevenvestigingen	X	-	-	-	-	-
		Prullenbak	X	-	-	-	-	-
		Relaties	X	X	-	-	-	-
		Rubrieken	X	-	-	-	-	-
		Schoolmededelingen	X	X	-	-	-	-
		Verzorgers	X	X	-	-	-	-
		Wachtwoordeisen	X	X	-	-	-	-
	Facturen	Afgenomen features	X	-	-	-	-	-
		Facturen	X	X	-	-	-	-
		Facturatiegegevens	X	-	-	-	-	-
	Schooltabellen	Absentieredenen	X	-	-	-	-	-
		Activiteitscategorieën	X	X	-	-	-	-
		Benoemingen	X	-	-	-	-	-
		Dienstverbanden	X	-	-	-	-	-
		Gezindtes	X	X	-	-	-	-
		Huisartsen	X	X	-	-	-	-
		Sociogramstellingparen	X	-	-	-	-	-
	Koppelingen	Certificaten	X	X	-	-	-	-
		Koppelingen	X	-	-	-	-	-
		Pasfoto's uploaden	X	X	-	-	-	-
	Toetsen en vakken	Eindtoetsgemiddelden	X	-	-	-	-	-
		Methodetoetsen	X	-	X	-	-	-
		Niet-methodetoetsen	X	-	X	-	-	-
		Vakken	X	-	-	-	-	-
	Digitaal rapport	Digitaal rapport	X	-	-	-	-	-
		Rapportcijferschalen	X	-	-	-	-	-
	Begeleiding	Ontwikkelingsperspectief	X	-	X	-	-	-
		Plancategorieën leerling	X	-	X	-	-	-
		Plancategorieën groep	X	-	X	-	-	-
	Map	Bestandscategorieën leerling	X	-	X	-	-	-
		Bestandscategorieën medewerker	X	-	X	-	-	-
		Notitiecategorieën leerling	X	-	X	-	-	-
		Notitiecategorieën medewerker	X	-	X	-	-	-
	Vragenlijsten	Vragenlijstsjablonen	X	-	-	-	-	-
Release notes			I	I	I	I	I	I

Toelichting rechtenstructuur

I = inzien
X = inzien / opvragen, toevoegen en wijzigen
(X) = inzien / opvragen en deels toevoegen en wijzigen
E = enkel eigen gegevens inzien / opvragen en wijzigen
- = niet beschikbaar

Bijlage 4 – Model Gebruikersovereenkomst

Gebruikersovereenkomst Stichting Openbaar Onderwijs Wijk bij Duurstede

[Onderwijsinstelling] te [Plaats], in deze vertegenwoordigt door [Naam], [functie], hierna te noemen werkgever
en
[Naam medewerk(st)er], personeelsnummer [nummer], werkzaam als [functie] bij [Onderwijsinstelling], hierna te noemen werknemer:
Verklaren dat zij een gebruikersovereenkomst voor bedrijfsmiddelen ICT, verder te noemen "apparatuur", voor [duur] zijn aangegaan. De navolgende voorwaarden zijn op deze overeenkomst van toepassing:

- Werkgever verstrekt aan werknemer de apparatuur ten behoeve van de uitoefening van de werkzaamheden van de dienstbetrekking.
- De apparatuur is eigendom van werkgever en wordt in bruikleen gegeven aan werknemer.
- Deze overeenkomst bepaalt de nadere gebruiksvoorwaarden waaronder werknemer de apparatuur kan gebruiken.
- Door ondertekening aanvaardt werknemer alle voorwaarden van deze overeenkomst.
-

1. Aard en uitvoering
Het type apparatuur en/of het abonnement wordt door werkgever vastgesteld en aangeschaft.

2. Rechten en plichten werknemer

a. Werknemer verklaart de apparatuur in goede staat te hebben ontvangen en zal deze niet aan derden ter beschikking stellen, verpanden of op enigerlei andere wijze vervreemden.
b. Werknemer is verantwoordelijk voor het in goede en representatieve staat houden van de apparatuur.
c. Tijdens een ziekteperiode van de werknemer van 6 weken of langer, moet de apparatuur ingeleverd worden bij werkgever.
d. Het is werknemer niet toegestaan zonder toestemming van de direct leidinggevende de apparatuur tijdens verlof mee te nemen naar het buitenland. Ook is bellen naar en vanuit het buitenland niet toegestaan.
e. Het is werknemer niet toegestaan zonder toestemming van de werkgever wijzigingen in de configuratie van de apparatuur aan te brengen.
f. Het is werknemer verboden de apparatuur te gebruiken voor activiteiten die in strijd zijn met de bedrijfsdoelstellingen of het aanzien van de werkgever schade (kunnen) berokkenen, dan wel de grenzen van betamelijkheid en fatsoen overschrijden.
g. Werknemer is op de hoogte dat werkgever het gebruik van de apparatuur door de werknemer controleert op het zakelijk gebruik van de apparatuur. Door ondertekening van deze overeenkomst stemt de werknemer in met deze controle. Tevens verklaart werknemer zicht bereid alle medewerking te verlenen die noodzakelijk is om het zakelijk gebruik te kunnen onderbouwen.

h. Werknemer verklaart zich akkoord dat indien werknemer heeft gehandeld in strijd met de bepalingen van deze gebruikersovereenkomst, eventueel daaruit voortvloeiende kosten zullen worden verhaald op werknemer.

3. Gebruik apparatuur

De werknemer wordt voor de uitoefening van zijn dienstbetrekking de apparatuur ter beschikking gesteld die werknemer voor minder dan € [bedrag] per jaar voor privé doeleinden gebruikt. Bij het belastbare loon van de werknemer wordt maandelijks een bedrag van € [bedrag] geteld voor het privégebruik van de mobiele telefoon.
De werknemer wordt voor de uitoefening van de dienstbetrekking een mobiele telefoon ter beschikking gesteld die werknemer uitsluitend voor zakelijke doeleinden dient te gebruiken.

4. Niet toegestaan gebruik

Het is werknemer niet toegestaan:

a. Sms-berichten te sturen naar of te ontvangen van commerciële nummers die niet werkgerelateerd zijn en tot (extra) kosten kunnen leiden, zoals reageren op radio- of tv-acties.
b. De verstrekte sim-kaart te gebruiken in een ander dan het verstrekte toestel.
c. Een andere sim-kaart in het verstrekte toestel te gebruiken dam de bij het verstrekte toestel behorende sim-kaart.
d. Gebruik te maken van bluetooth anders dan voor het verbinden met een headset of carkit. Bij gebruik van bluetooth moet de keuze 'verborgen' worden ingesteld.
e. Het toestel uit handen te geven of uit te lenen aan personen van buiten de organisatie.

5. Diefstal en beschadiging

a. Werknemer dient afdoende beschermingsmaatregelen te treffen, zoals periodiek wijzigen van wachtwoorden en dergelijke, ter bescherming van gegevens op de apparatuur.
b. Werknemer dient alle zorgvuldigheid in acht te nemen ter voorkoming van beschadiging, diefstal of verlies van de apparatuur.
c. In geval van schade of diefstal van de apparatuur is werknemer verplicht dit zo spoedig mogelijk, doch uiterlijk binnen 24 uur bij werkgever te melden. Als contractant draagt werkgever het risico voor misbruik na diefstal, mits aan het hiervoor gestelde is voldaan.
d. Werknemer kan aansprakelijk worden gesteld voor verlies van of schade aan de apparatuur ontstaan door verwijtbare nalatigheid of onachtzaamheid. Kosten voor herstel of vervanging kunnen in dat geval worden ingehouden op het salaris van medewerker.

6. Termijn van gebruik

a. Werknemer dient de apparatuur binnen de afgesproken bruikleentermijn dan wel bij beëindiging van het dienstverband of functieverandering op eerste verzoek in volledige staat te retourneren. Bij verzuim hiertoe, verbindt werknemer zich tot betaling van de rest(boek)waarde van de apparatuur aan werkgever.
b. Indien werknemer na het einde van de bruikleenovereenkomst of na opzegging hiervan door werkgever niet onmiddellijk voldoet aan een verzoek van werkgever tot teruggave van de apparatuur, verbeurt werknemer een boete van € [bedrag] voor iedere dag, dat werknemer, na bij aangetekende brief door werkgever vermaand te zijn, aan zijn verplichtingen niet voldoet.
c. Indien één van de genoemde gevallen in deze gebruikersovereenkomst zich voordoet, is werkgever bevoegd een geschil betreffende de teruggave van de apparatuur aan het oordeel van de President van de arrondissementsrechtbank te [Plaats], rechtsprekende in kort geding, te onderwerpen.
d. Door ondertekening van deze overeenkomst verklaart werknemer dat hij gevolgen van deze overeenkomst heeft begrepen en zich daarmee akkoord verklaart.

Aldus verklaard, opgemaakt in tweevoud en ondertekend te [Plaats],
[Naam onderwijsinstelling]

.....	.....
Naam:	Naam:
Datum:	Datum:

Bijlage 5 - Wachtwoordbeleid

Wachtwoorden zijn voor computer toegangen en informatie wat sleutels zijn voor je huis. Je huis laat je ook niet zomaar open voor iedereen, toch? Daarom zijn wachtwoorden heel belangrijk want ze schermen informatie en computersystemen af .
Op scholen zijn veel werkplekken die voor iedereen (kinderen, ouders, externen) toegankelijk zijn. Een wachtwoord zorgt ervoor dat onbevoegden geen toegang tot privacygevoelige en vertrouwelijke informatie kunnen krijgen.
Om ervoor te zorgen dat de privacy gewaarborgd blijft, zijn er een aantal regels opgesteld om wachtwoorden te beschermen:

- Het wachtwoord mag nooit doorgegeven worden aan collega's, vrienden, familie of onbekenden. Een wachtwoord is strikt persoonlijk.
- Het is een goede gewoonte om je wachtwoorden voor alle toepassingen geregeld te wijzigen. Medewerkers worden verplicht om het Google account Office 365 wachtwoord minstens één keer per jaar te wijzigen.
- Het wachtwoord is minstens 1 en maximaal 24 karakters lang.
- Er moet minstens één hoofdletter, één kleine letter en één cijfer in voorkomen.
- Het mag niet makkelijk te raden zijn aan de hand van persoonlijke informatie zoals naam, adres, telefoonnummer of geboortedatum.
- Het wachtwoord mag nergens zichtbaar opgeschreven worden. (Dit houdt o.a.in dat een gebruikersnaam en wachtwoord van een medewerker of leerling niet op een papiertje staan, wat vervolgens op de monitor of onder het toetsenbord van de werkplek is geplakt).Ook niet het wachtwoord opslaan in notities van je telefoon.
- Gebruik je wachtwoord niet voor een tweede keer. Verzin echt elke keer een ander wachtwoord.
- Gebruik niet hetzelfde wachtwoord voor school en privé doeleinden
- Het is ook niet toegestaan om het wachtwoord ergens automatisch op te slaan.
- Bij vermoeden van misbruik wijzig je zo snel mogelijk je wachtwoord en meldt je je vermoeden aan de Security Officer

Als een wachtwoord niet aan bovenstaande eisen voldoet, wordt het wachtwoord z.s.m. aangepast door de medewerker.
Als de medewerker het wachtwoord niet zelf kan aanpassen, vraagt hij om hulp bij de ICT'er. Lukt het aanpassen niet dan wordt dit gedaan door de systeembeheerder of de boven schoolse medewerker ICT.
Leerlingen (groepen) krijgen een wachtwoord via de systeembeheerder. Aanpassingen kunnen gedaan worden door de leerling zelf in overleg met de leerkracht of door de leerkracht of ICT'er van de school.
De leerlingen worden bewust gemaakt van wachtwoordbeheer tijdens de lessen mediawijsheid.

Tot slot
Het is belangrijk om je af te melden/uit te loggen bij zowel de applicatie als de pc, als je wegloopt van de werkplek. Uiteraard kun je ook de computer vergrendelen. Dit doe je:

- door Windows+L in te drukken (de Windows-toets is de toets met het vlaggetje in de omgeving van de spatiebalk).
  Je scherm wordt dan vergrendeld en is alleen weer te benaderen door je aan te melden.

Bovenstaande is belangrijk omdat allerlei privacygevoelige informatie geraadpleegd kan worden op werkplekken die voor iedereen (kinderen, ouders, externen) toegankelijk zijn.

Extra informatie

Wachtwoorden bewaren

Veel mensen worden tureluurs van alle wachtwoorden die ze moeten aanmaken en vervolgens onthouden. Gelukkig zijn er hulpmiddelen voor het opslaan en bewaren van wachtwoorden. Bijvoorbeeld het gebruik van een wachtwoordmanager.
Een wachtwoordmanager werkt als een kluis. In die kluis bewaart u uw, uiteraard sterke, wachtwoorden. Deze kluis is digitaal. Toegang tot de kluis krijgt u met een 'sleutel'. Deze digitale sleutel is het enige wachtwoord dat u echt nog moet onthouden.
Hiermee krijgt u toegang tot al uw bewaarde wachtwoorden in de kluis. De wachtwoordmanager vult automatisch uw wachtwoord in na de eerste keer inloggen op een site. Na gebruik zet u de manager uit, en om hem weer te gebruiken hebt u alleen uw 'sleutel' nodig om op alle sites automatisch ingelogd te worden.

LastPass

Een goede Nederlandstalig wachtwoordmanager is LastPass. Dit programma is zowel op Windows, als de Mac en mobiele apparaten (tablets en smartphones) te gebruiken.
U installeert het programma en zet een invoegtoepassing in uw browser. Dit is eigenlijk een extra knop waarmee u toegang hebt tot verschillende functies van LastPass terwijl u aan het surfen bent.
Logt u in op een website, dan vraagt LastPass of het uw wachtwoord moet opslaan. Doet u dit, dan wordt het wachtwoord door LastPass bewaard en hoeft u de volgende keer uw wachtwoord niet meer in te vullen. En moet u ergens een nieuw wachtwoord aanmaken, dan kan LastPass dat wachtwoord ook voor u bedenken. Een sterker wachtwoord kunt u zelf bijna niet maken. Het nadeel hiervan is wel dat u dan écht afhankelijk bent van het programma.
De gratis versie van LastPass kunt u op meerdere computers gebruiken. U kunt het programma op verschillende computers installeren. Wilt u ook op uw smartphone of tablet toegang tot de wachtwoorden die u in LastPass hebt opgeslagen, dan betaalt u hier negen euro per jaar voor met LastPass Premium. U kunt dan een LastPass app downloaden waarmee u het internet op gaat. Surft u via deze app, dan worden uw wachtwoorden ingevuld door LastPass.
Hoe u de gratis versie van het programma gebruikt leest u in 'Last Pass gebruiken'.

Waarom kiezen voor complexe wachtwoorden?

Een wachtwoord mag niet gemakkelijk te raden zijn door persoonlijke informatie (bv. naam, achternaam, geboortedatum, naam kinderen, ...) als wachtwoord te kiezen, of door een logische combinatie van karakters te kiezen (bv. aaa, abc, 1234, azerty, ...)
Een wachtwoord complex maken is essentieel omdat anderen met slechte bedoelingen hierdoor minder snel het wachtwoord kunnen raden. Een sterk wachtwoord verkleint het risico dat een ander met jouw gebruikersnaam en wachtwoord kan inloggen. Een gemakkelijk te raden wachtwoord zet de deur op een kier voor misbruik. Wanneer anderen je wachtwoord kunnen raden, kunnen er frauduleuze activiteiten uitgevoerd worden vanuit jouw naam.
Complexe wachtwoorden zijn dus wachtwoorden die bestaan uit niet-logische verbanden met minstens één hoofdletter, één kleine letter en één cijfer. Daarnaast kan je het wachtwoord nog complexer maken door nog een symbool (&, -, *, ...) toe te voegen.

Hoe kan ik een sterk wachtwoord onthouden?

Om sterke wachtwoorden te onthouden bestaan wat trucjes, want de kunst is om een niet te raden wachtwoord te verzinnen dat je toch zelf kan reconstrueren.

- Neem een zin die voor jou makkelijk te onthouden en betekenisvol is. Kies hiervoor niet een zin als ik heb een blauwe Opel als je een blauwe Opel hebt. Maar denk aan zinnen als ik heb een roze olifant.
- Neem van elk woord telkens de eerste letter of gebruik de hele zin als wachtwoord.
- Voeg symbolen en hoofdletters toe .

Gebruik verschillende wachtwoorden voor verschillende toepassingen Omdat het internet nu eenmaal een anonieme en onbetrouwbare wereld is en omdat de beveiliging van websites met hun toegangscontroles niet altijd even goed is opgezet, is het belangrijk om verschillende wachtwoorden te gebruiken.
Kies daarom verschillende wachtwoorden voor verschillende situaties:

- Je Google account Office 365 geeft je toegang tot je mail, agenda en drive. Het is belangrijk dat je dit account goed afschermt, dus je neemt een sterk, uniek wachtwoord. *Ook je thuisbankieren scherm je af met een sterk, uniek wachtwoord. Met je bankverrichtingen wil je geen enkel risico nemen!*
- Je Windows-computer scherm je af met een sterk wachtwoord, zodat een toevallige voorbijganger niet kan binnenbreken op je computer.
- Naast je Google account Office 365 heb je nog een aantal accounts voor applicaties die privacygevoelige informatie bevatten. Ook deze accounts scherm je af met een sterk wachtwoord.
- Je registreert je af en toe op een site, om binnen te mogen op die site, maar de site houdt geen persoonlijke informatie over je bij. Je gebruikt voor meerdere sites hetzelfde wachtwoord, zodat je dit makkelijk kunt onthouden.

Draag zorg voor je wachtwoorden

Er zijn heel wat goede gewoontes om zorgvuldig om te gaan met wachtwoorden.

- Zoek geen manieren om het inloggen te automatiseren of het ingeven van een wachtwoord te omzeilen - het wachtwoord is er voor je veiligheid. *Je laat thuis toch ook niet de sleutels op de deur zitten wanneer je er niet bent?*
- Zorg ook voor enige vorm van fysieke beveiliging. Het volstaat niet om een wachtwoord op je computer te plaatsen, als je je computer open en bloot op je werkplek laat staan terwijl je een kop koffie haalt. Maak er een gewoonte van om je computer elke keer te vergrendelen wanneer je je werkpost verlaat. Onder Windows kan dit eenvoudig door Windows+L in te drukken (de Windows-toets is de toets met het vlaggetje in de omgeving van de spatiebalk).
- Wanneer je misbruik vermoedt, of je denkt dat iemand je wachtwoord meegelezen heeft, verander je je wachtwoord in een nieuw, uniek wachtwoord en meldt je vermoeden bij de Security Officer (SO)
- Wanneer je - bv. op vakantie - je e-mail leest op een publieke computer, verander dan ook achteraf je wachtwoord. Je weet immers niet welke programma's op de publieke computer op de achtergrond draaien; een programma houdt misschien ijverig alle ingetikte wachtwoorden bij.
- Geef je wachtwoord enkel op een beveiligde webpagina in. Beveiligde webpagina's lopen over een https-verbinding (s voor secure). Bij https-verbindingen worden de wachtwoorden geëncrypteerd zodat deze voor een kraker veel moeilijker te lezen zijn. Bij gewone http-verbindingen zijn wachtwoorden gewoon leesbaar voor iedereen die het netwerkverkeer aftapt.

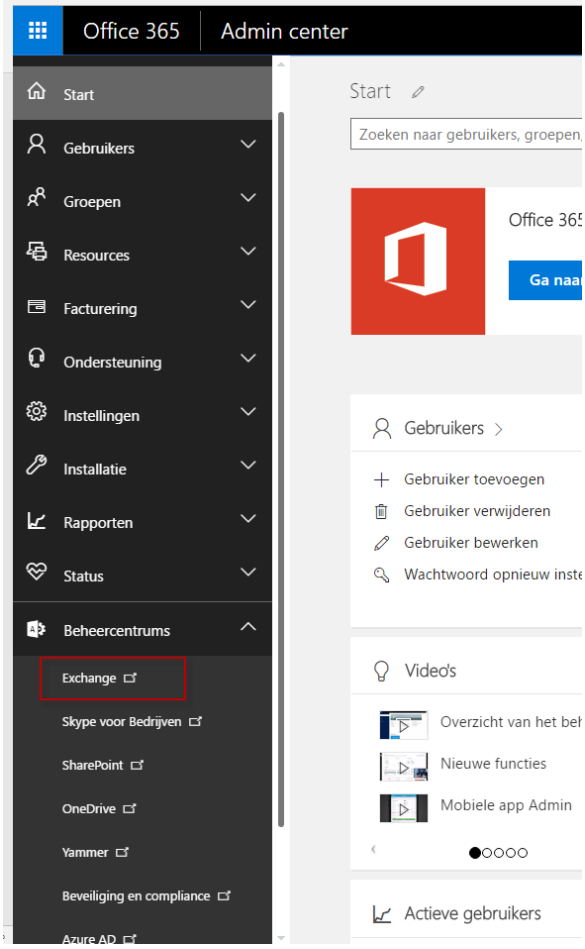
Een beveiligde webpagina herken je aan:

- het adres, bv. https://duo.nl (s staat voor secure).
- een slotje dat in de meeste browsers onderaan of in de adresbalk verschijnt
- het "certificaat" dat je bij de meeste internetprogramma's kan opvragen

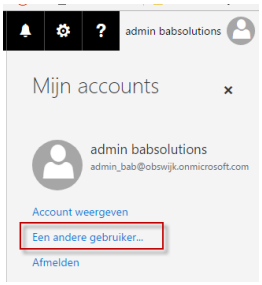
Office 365 mobiel apparaat op afstand wissen

Stap 1. Log op de Office 365 omgeving in als beheerder:
https://login.microsoftonline.com of obswijk.sharepoint.com → beheer

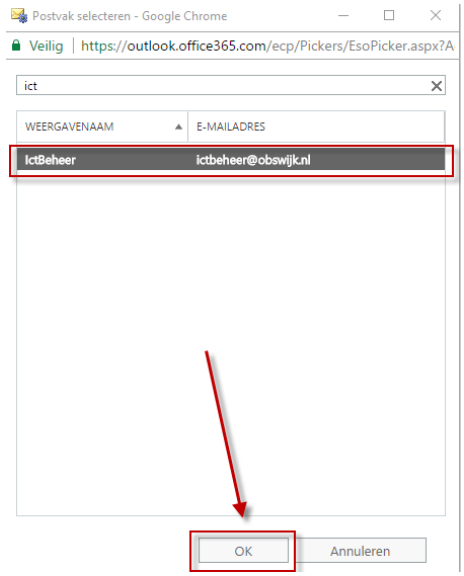
Stap 2. Kies bij "Beheer" voor "Exchange" (onder beheercentrums), een nieuw venster opent:



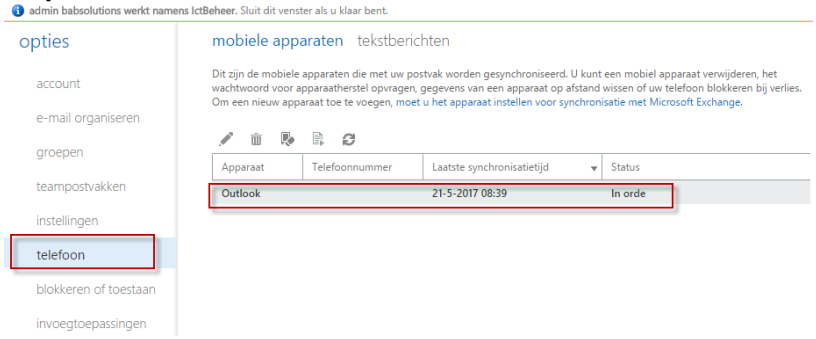
Stap 3. Klik rechts bovenin op het profiel icoon, kies "Een andere gebruiker":



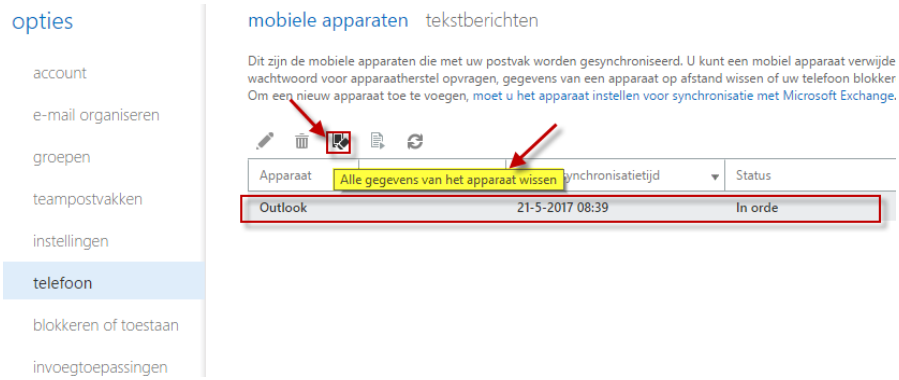
Stap 4. Zoek en selecteer de gebruiker. Een nieuw venster opent:



Stap 5. Kies in het menu voor "telefoon":



Stap 6. Selecteer het te wissen apparaat, kies voor "Alle gegevens van het apparaat wissen".



Stap 7. Het "Wis" commando wordt naar het apparaat gestuurd en deze stelt zich vervolgens terug naar fabrieksinstellingen.