OPENBAAR VOORTGEZET ONDERWIJS ZAANSTAD

Wegwijzer Privacy

Vooraf

Hoe OVO Zaanstad met privacy om gaat is terug te lezen op de privacy pagina onder 'Mijn werk' op intranet van OVO Zaanstad. Hiermee zijn we er (nog) niet. De protocollen dienen vertaald te worden naar de praktijk van alle dag van de scholen en van OVO Service. Deze wegwijzer helpt daarbij door een aantal praktische veelvuldige vragen te beantwoorden. Mocht jouw vraag er niet tussen staan, neem dan contact op met de privacy officer van je school.

Waar en hoe bewaar ik persoonsgegevens?

Verwerk persoonsgegevens zoveel mogelijk digitaal in de daarvoor aangewezen bewaarplaatsen.
Leerlinggegevens worden zoveel mogelijk digitaal opgeslagen, geraadpleegd en bewerkt in ons leerlingadministratie en -volgsysteem. Dit geldt ook voor gegevens die via ouders/verzorgers en/of externen worden ontvangen. Deze kunnen in de logboekbestanden worden opgeslagen. Personeelsgegevens van alle medewerkers worden zoveel mogelijk digitaal opgeslagen in het centrale personeelsadministratiesysteem. Daarnaast worden op school nog ondersteunende systemen gebruikt voor personeels- en formatieplanning voor docenten. Er worden géén persoonsgegevens op USB-sticks bewaard.

Gegevens die op papier aangeleverd worden, worden gescand en aan bovengenoemde systemen toegevoegd. Vergeet niet om de scan van je eigen computer te verwijderen en het papieren origineel te vernietigen.

Formuleer gegevens die je vastlegt over een persoon zorgvuldig en professioneel.
Ouders en medewerkers hebben het recht om hun dossier of het dossier van hun kind in te zien. Zorg ervoor dat de gegevens zodanig zijn geformuleerd dat dit kan.

Gebruik voor de verwerking van leerlinggegevens bij voorkeur een computer van school.
Moet je persoonsgegevens downloaden en bewerken op je computer? Doe dit alleen op een beveiligde computer en bij mobiele apparatuur die voorzien is van encryptie, bij voorkeur een computer van school. Verwijder de bestanden na gebruik van je computer.

Gebruik je toch een computer of device buiten de school of thuis? Zorg dan dat anderen (bijv. familieleden) niet bij jouw werkbestanden kunnen komen.

Ga na welke afspraken er binnen de school gemaakt zijn voordat je persoonsgegevens uitwisselt met derden.
Voor het uitwisselen van persoonsgegevens met externen, zoals bijvoorbeeld de arbo- of schoolarts, de gemeente, jeugdzorg of een schoolbegeleidingsdienst, is soms toestemming nodig van ouders of van de leerlingen zelf (≥ 16 jaar).

Weet je niet of voor jouw specifieke geval toestemming nodig is? Neem dan contact op met de privacy officer van je school of stel je vraag aan de functionaris gegevensbescherming fg@ovo-zaanstad.nl.

Zorg dat je de toestemming registreert en houd daarbij ook rekening met de verdeling van het ouderlijk gezag (zie gedragsprotocol informatievoorziening gescheiden ouders).

NB. Ook al vragen derden om de levering van persoonsgegevens via email, telefoon of via de balie, je bent vaak niet verplicht om ze te geven. Controleer bij het verzamelen of delen van persoonsgegevens of hiervoor een wettelijke grondslag bestaat aan de hand van de Vuistregels Privacy. Tip: Bekijk in het privacyreglement met welke partijen gegevens (mogen) worden uitgewisseld.

Welke informatieplicht heb je?
Ouders en leerlingen ≥ 16 jaar worden voorafgaand aan de verwerking geïnformeerd over het verwerken van diens gegevens, ook als deze van derden worden verkregen. Meer hierover kan je vinden in de privacyreglementen die op de privacypagina op intranet zijn gepubliceerd.

Wat communiceer ik aan wie?
Iedereen heeft alleen inzage in die gegevens die hij/zij nodig heeft voor het werk. Dat betekent dat informatie die relevant is voor enkelen (bijvoorbeeld een adreswijziging of een ziekmelding) bijvoorbeeld niet in een nieuwsbrief aan iedereen gestuurd kunnen worden tenzij er met iedereen expliciete afspraken over gemaakt zijn? Dat betekent ook dat een docent alleen toegang heeft tot gegevens van zijn klas en niet bij voorbaat tot gegevens van andere klassen om bijvoorbeeld waarneming mogelijk te maken. Toegang mag alleen voor de periode van waarneming!

Mogen anderen jouw mail inzien?
Medewerkers mogen niet zomaar de mailbox van een collega inzien, bijvoorbeeld als deze ziek is of op vakantie. Degene van wie de mailbox is moet hier toestemming voor geven. Kan het echt niet wachten of kan toestemming vragen niet meer? Dan moet op managementniveau de afweging worden gemaakt of in dat specifieke geval de privacy van de medewerker minder belangrijk is dan het belang van de school of afdeling om toegang te krijgen tot bepaalde gegevens of documenten.

Hoe en wat communiceer ik online?
Maak gebruik van een link naar het digitaal administratiesysteem om persoonsgegevens uit te wisselen met collega's.
Verstuur persoonsgegevens bij voorkeur niet per mail, maar verstuur een link naar de online bewaarplaats van de benodigde gegevens.

Vraag ouders om toestemming om een (privé)account aan te maken voor online diensten.
In de onderwijs worden online tools ingezet, bijvoorbeeld een quiz app of een site die ondersteunt bij het woordjes leren voor vreemde talen.

Soms moeten de leerlingen hiervoor zelf een account aanmaken. Let dan op dat leerlingen jonger dan 16 jaar toestemming hebben van hun ouders/verzorgers om zo'n (privé)account aan te maken.

Deel over leerlingen, ouders of collega's 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.

Gebruik de accounts die door de school worden beheerd als je met anderen wil communiceren via e-mail of social media.
Formuleer je boodschap hier professioneel en zorgvuldig.

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 op de privacypagina op intranet.

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. Privémeningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de school en/of het bestuur. Wees je ervan bewust dat gepubliceerde uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na het verwijderen van het bericht.

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.

Wanneer je een bericht stuurt met belangrijke en/of gevoelige informatie naar (een groep) ouders/verzorgers, wees dan zorgvuldig met het invoeren van e-mailadressen.
Het kan heel makkelijk dat een mail naar de verkeerde persoon wordt gestuurd, pas daarom op met wat en aan wie je iets stuurt.

Gebruik sociale media en berichten apps waaronder whats app alleen met toestemming
Als een school leerlingen gebruik wil laten maken van sociale media of berichten apps, dan moet er voor leerlingen jonger dan 16 jaar vóóraf apart toestemming worden gevraagd aan de wettelijk vertegenwoordigers (ouders). Het is van belang vóóraf een goede afweging te maken om social media wel of niet in te zetten in (het kader van) het onderwijs en vooraf te bedenken wat te doen als ouders géén toestemming geven.

Hoe houd ik indringers op afstand?

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.

Bewaar laptops of tablets altijd op een veilige, afgesloten plek, zeker tijdens vakantieperiodes.
Maak elkaar er op attent als je een laptop of tablet onbeheerd ziet liggen. Als je computer gestolen wordt, heeft dat gevolgen voor de school en de leerling. Neem in dat geval direct contact op met de privacy officer van je school.

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).

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  - en L-toets kun je je computer makkelijk vergrendelen. 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. Maar ook geef anderen niet jouw code van de printer.

Zet het 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 notificatiefunctie van je e-mail uit, zodat er tijdens je les geen meldingen op het bord binnen komen die leerlingen kunnen zien, maar niet voor hun ogen bestemd zijn.

Laat je wachtwoorden van digitale (administratie)systemen met persoonsgegevens niet onthouden door je internetbrowser. En schrijf je logingegevens nooit op en log uit!
Maak gebruik van wachtwoordkluisjes, zoals Last Pass of True Key. Zonder dat je er erg in hebt, klik je de optie 'wachtwoord onthouden' in je browser aan. Heel makkelijk als je vaak moet inloggen, maar iemand anders kan dan dus ook inloggen.

Houd je logingegevens altijd voor jezelf, ook al vragen anderen aan je om ze te delen.
Je login is in feite een sleutel om toegang te krijgen tot de informatie die alleen voor jou toegankelijk moet zijn. Daarnaast herkent het systeem jou door je login, zodat het kan bijhouden wie welke gegevens heeft toegevoegd of gewijzigd.

Welke gegevens mag ik aan derden geven?
In principe mag je geen gegevens aan derden geven of verstrekken zonder toestemming van de ouders of leerling ≥ 16 jaar. Dat geldt voor digitale gegevens, papier maar ook om beeld- & videomateriaal. Soms is het wettelijk bepaald dat dat wel mag. Het is van belang om altijd eerst te checken of degene die jou om de gegevens vraagt, deze wel zonder toestemming mag hebben. De gemeente vraagt soms om informatie van leerlingen voor gemeentebeleid. Ook belt soms de leerplichtambtenaar voor een specifiek geval. Hoewel dit officiële instanties zijn, hebben zij niet altijd recht op informatie. Veel van de informatie die de gemeente nodig heeft en waar zij recht op heeft, krijgt zij via DUO. Dit geldt ook voor de GGD.

Kortom, het is dus belangrijk eerst te checken of zij de gegevens wel mogen krijgen op basis van een wet. Of dat de gegevens al via OVO Zaanstad worden verstrekt. Is dit niet het geval, dan is de vraag of je de gegevens wel moet willen geven. Wil je dit toch doen, dan is toestemming van de ouders nodig.

Welke rechten hebben ouder, leerlingen en medewerkers?
Transparantie is een belangrijke privacy-waarde. We betrekken ouders en leerling actief. We leggen uit, vertellen welke gegevens we willen vastleggen of verstrekken aan het samenwerkingsverband, of een derde, en waarom. Dit geldt ook voor de informatieoverdracht tussen scholen bij een overstap. We stellen ouders en leerling in staat om bezwaren te uiten en hun rechten uit te oefenen. Deze rechten zijn vastgelegd in de wet. De betrokkenen hebben de volgende rechten:

- **Recht op informatie** houdt in dat de leerling en/of zijn ouders (de betrokkene) vooraf door de school in begrijpelijke taal actief en laagdrempelig worden geïnformeerd over welke gegevens met welk doel worden verwerkt en wat de rechten van de leerling zijn. Hiervoor kan de folder voor ouders worden gebruikt. Deze vind je op de privacypagina van intranet.
- **Recht op inzage in** en **correctie van** de persoonsgegevens. De betrokkene heeft het recht op inzage van zijn gegevens en het verbeteren of aanvullen van ontbrekende of verkeerd vastgelegde persoonsgegevens.
- **Recht op verwijdering van** de persoonsgegevens die niet (langer) nodig zijn om de vastgestelde doelen te behalen. Het gaat alleen om gegevens die niet noodzakelijk zijn, of als het opslaan van die gegevens in strijd is met de wet. Een

leerling kan dus niet vragen om zijn ‘1’ voor een overhoring te 'verwijderen’ op grond van privacywetgeving.

- **Recht van verzet tegen verwerking** van persoonsgegevens bij de grondslag gerechtvaardigd belang , of verzet tegen direct marketing en profilering. De betrokkene kan verzet instellen tegen een verwerking van zijn persoonsgegevens die plaats vond op grond van een gerechtvaardigd belang. We maken een afweging van het privacybelang van de leerling, tegenover het belang van de school om gegevens wél te gebruiken.
- De leerling en/of zijn ouders hebben het **recht** om bij toestemming, ook een beperkte toestemming te geven of toestemming te onthouden voor een onderdeel van de verwerking (**granulaire toestemming**).
- De leerling en/of zijn ouders hebben het **recht** dat verbeteringen, aanvullingen of verwijderingen aan alle andere partijen worden doorgegeven aan wie een organisatie de persoonsgegevens van betrokkene heeft verstrekt;
- Het recht op ‘**bevriezing van de verwerking**’ van zijn gegevens
- De betrokkene heeft het ‘**recht om te worden vergeten’** door het volledig wissen van de persoonsgegevens, tenzij er een wettelijke bewaarplicht geldt of het verwijderen in strijd is met de vrijheid van meningsuiting. Voor het onderwijs is dit recht minder relevant omdat we veel wettelijke bewaartermijnen gelden.

Als een ouder gebruik wil maken van zijn rechten dan dient hij hiertoe een schriftelijk verzoek in bij OVO Zaanstad, o.v.v. privacy. Als een ouder een klacht in wil dienen over de wijze waarop OVO Zaanstad en de aangesloten scholen omgaan met privacy, dan kan hij/zij zich wenden tot de functionaris gegevensbescherming van OVO Zaanstad (fg@ovo-zaanstad.nl).

Wanneer is er sprake van een beveiligingsincident of datalek?

Mochten persoonsgegevens (hetzij digitaal, hetzij schriftelijk, hetzij mondeling) nu toch zonder toestemming aan een derde zijn verstrekt, onbedoeld zijn verwijderd of kwijt zijn geraakt, of zijn we gehackt neem dan direct contact op met de privacy officer van jouw school. Als het beveiligingsincident een datalek betreft, dan dient deze namelijk binnen 72 uur aan de autoriteit persoonsgegevens gemeld te worden!

Tot slot!

Wat *niet* te doen bij de verwerking van privacygevoelige informatie:

- Niet afdrukken tenzij strikt noodzakelijk
- Niet versturen via de mail (of versleuteld, of met wachtwoord beveiligde bijlage)
- Geef je inloggegevens nooit aan iemand anders
- Bewaar je inlog niet op papier
- Bewaar je inlog niet in een eenvoudig leesbaar bestand.

Wat *wel* te doen bij de verwerking van privacygevoelige informatie:

- Gebruik encryptie voor de mobiele apparatuur als USB, laptop en mobiele telefoon (bitlocker, vraag de ICT-beheerder van de school wat te doen)
- Sla de informatie op binnen een veilig systeem (AFAS, Magister, Office 365 of netwerkschijf van de school of OVO Zaanstad)
- Raadpleeg de informatie via deze systemen (AFAS, Magister, Office 365 of netwerkschijf van de school of OVO Zaanstad)
- Beveilig gevoelige bestanden met een wachtwoord
- Sla uitsluitend strikt noodzakelijke informatie op
- Gebruik als leidinggevende en/of beheerder tweeweg authenticatie ofwel een token (AFAS, Magister, Office 365)
- Zorg ervoor dat mobiele apparaten voorzien zijn van een pincode of vergelijkbaar
- Sla papieren stukken achter slot op

- Vernietig papieren stukken wanneer deze niet meer nodig zijn. Je kunt de termijnen terugvinden in ons dataregister op intranet.
- Vergrendel de computer met ( +L) wanneer deze onbeheerd wordt gelaten
- Gebruik een wachtwoordkluis (bijvoorbeeld KeePass) voor het beheren van je wachtwoorden
- Laat mobiele apparatuur niet op een diefstalgevoelige plek achter.
- Log in magister in als klasdocent zodat je niet meer rechten krijgt dan nodig om de les te geven. die je voor de les nodig hebt.