



Sancta Maria
HAVO • ATHENEUM • GYMNASIUM



Privacy-AVG
informatie

Inhoudsopgave



P.4 Privacy en de AVG

P.7 Veilig omgaan met persoonsgegevens?

P.12 Bewaartermijnen op school

P.14 Phishing

P.17 Foto en Film op school

P.20 Apps en tools op school

- alle privacy documenten voor medewerkers vind je in de Teamstegel medewerkers/ privacy

Met dank aan 'privacy op school' voor de ontwikkeling van de stroomschema's en de infographics en de mogelijkheid om deze te mogen verwerken in dit informatieboekje.

Welkom

Op Sancta verwerken (verzamelen, opslaan en gebruiken) wij persoonsgegevens van leerlingen, ouders en medewerkers. Dit is noodzakelijk voor het organiseren van het onderwijs en inherent aan werkgeverschap. Vanzelfsprekend gaan wij zorgvuldig met deze gegevens om en houden we ons aan de privacywetgeving.

In dit privacy-informatieboekje staat beschreven hoe de omgang met persoonsgegevens eruitziet en hoe iedereen eraan kan bijdragen. Zo kunnen we de privacy van medewerkers, leerlingen en overige betrokkenen zo goed mogelijk waarborgen. Dit privacy-boekje is dynamisch en zal aangepast worden als de wetgever of de praktijk daarom vraagt.

Heb je vragen of tips voor informatie die jij graag opgenomen ziet in dit privacy-boekje? Neem dan gerust contact op met je teamleider of onze privacy officer Susanne de Wit via privacy@sanctamaria.nl.

In dit privacy boekje wordt soms de afkorting FG gebruikt, hiermee wordt de privacy officer bedoeld.





Privacy en de AVG

Er wordt door bedrijven veel informatie over ons verzameld en vastgelegd: camerabewaking, koopgedrag, locatiegegevens, medische gegevens, onze politieke voorkeur, etc. Met de komst van sociale media verstrekken we zelf bedoeld en onbedoeld ook veel informatie over onszelf en anderen. Deze gegevens kunnen worden verzameld en vervolgens worden gekoppeld, gebruikt of doorverkocht. Want onze gegevens zijn veel geld waard.

Regels rond het gebruik van persoonsgegevens zijn in 2018 vastgelegd in de Algemene verordening gegevensbescherming (AVG), en eerder in de Wet bescherming persoonsgegevens.

De AVG schrijft het volgende over privacy:

- Privacy is een grondrecht en een voorwaarde om vrij te kunnen zijn in wie je bent en wat je doet.
- We houden zelf regie over onze gegevens: één openbare foto waarop iemand als dronken tiener te zien is, is niet toekomstbepalend.
- We worden niet continu gevolgd, onze medische gegevens zijn veilig en we kunnen genomen besluiten die op ons betrekking hebben aanvechten.
- We hebben zeggenschap over onze eigen persoonsgegevens.

De AVG beschermt onder meer de privacy van leerlingen, medewerkers, ouders en overige personen.

De AVG beschermt onder meer de privacy van leerlingen, medewerkers, ouders en overige personen. Er zijn afspraken over hoe scholen moeten omgaan met persoonsgegevens en privacygevoelige informatie. Ouders van leerlingen behartigen op het terrein van privacy de belangen van hun kind tot het 16e levensjaar. Daarna hebben leerlingen zelf de zeggenschap over hun persoonsgegevens.

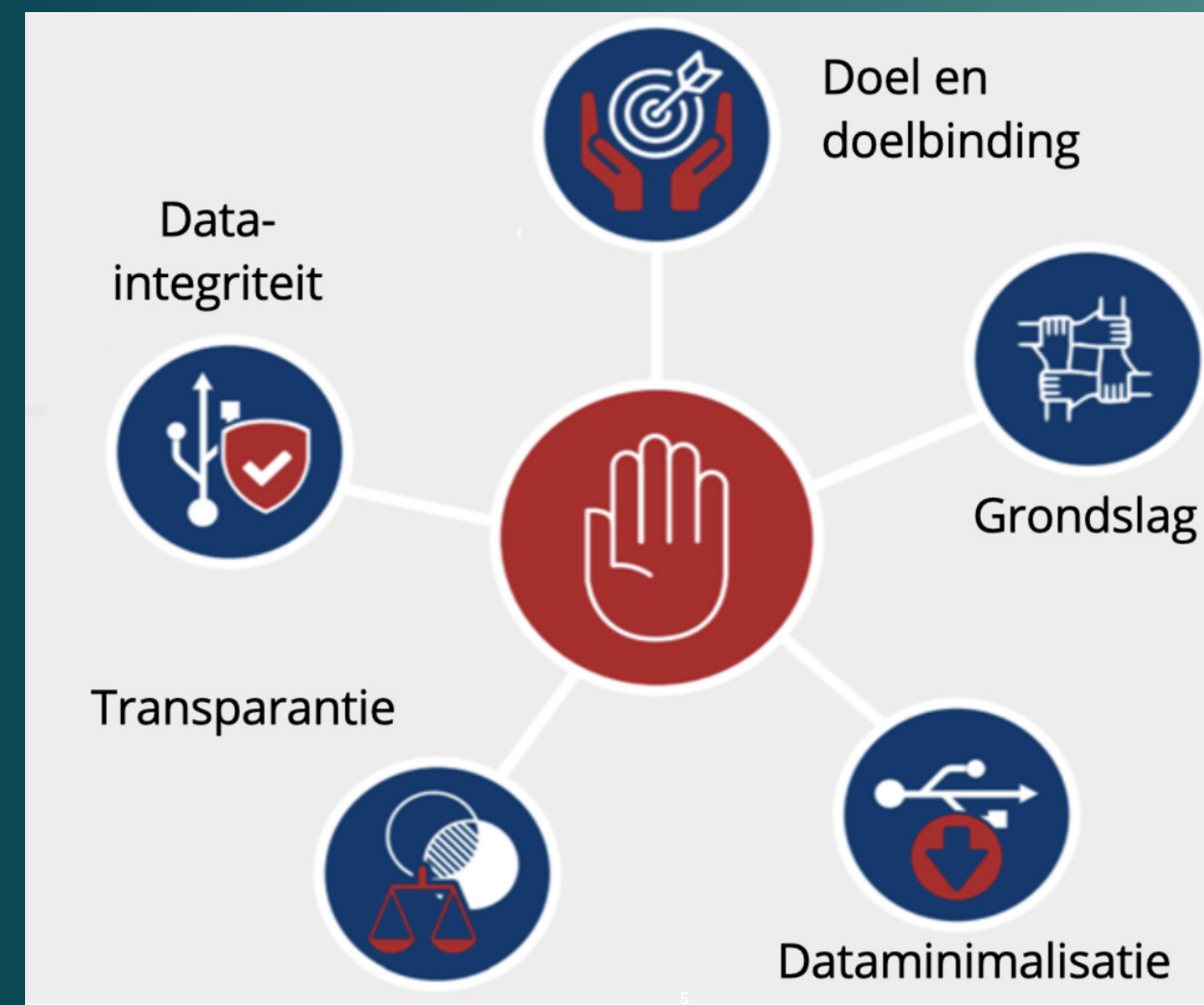
De AVG geeft de kaders waarbinnen persoonsgegevens door de school verzameld, opgeslagen en gebruikt mogen worden. Het is belangrijk te beseffen dat het niet zo is dat de AVG alles onmogelijk maakt. Een school is er om onderwijs te geven, en in dat kader mag de school dan ook gerust persoonsgegevens verwerken (verzamelen, opslaan en gebruiken).

De school mag persoonsgegevens ook doorgeven wanneer er sprake is van een wettelijke plicht. Denk aan de leerplichtambtenaar, de gemeente of Veilig Thuis. Voor het doorgeven van bepaalde gegevens moet echter altijd voorafgaande toestemming worden gevraagd en gegeven. Het gaat dan vaak om gegevens die (net) niet binnen de onderwijstaak vallen. Denk aan het maken van klassenfoto's of video's van leerlingen.

Vuistregels voor omgaan met persoonsgegevens op school

Wij hanteren vijf vuistregels. In deze vijf vuistregels worden de belangrijkste uitgangspunten voor het verantwoord omgaan met persoonsgegevens samengevat.

1. Doel en doelverbinding: we mogen alleen gegevens verwerken (verzamelen, opslaan en gebruiken) voor een specifiek doel. Als dat doel bereikt is, mogen gegevens niet verder verwerkt worden.
2. Grondslag: we moeten nagaan of gegevens gebruikt mogen worden voor het onderwijs. Zijn de gegevens bijvoorbeeld noodzakelijk voor het goed uitvoeren van het onderwijs dan hoef je geen toestemming te vragen. In alle andere gevallen vaak wel.
3. Dataminimalisatie: we verwerken (verzamelen, opslaan en gebruiken) alleen hoogstnoodzakelijke gegevens.
4. Transparantie: we informeren leerlingen, ouders, medewerkers en derden waar we de gegevens voor nodig hebben en waarvoor we de gegevens gebruiken, hoe en hoelang we ze bewaren.
5. Data integriteit: de gegevens die we bewaren moeten kloppen.



Wat zijn persoonsgegevens?

Persoonsgegevens zijn gegevens die iets over iemand zeggen of naar iemand terug te herleiden zijn. Denk hierbij aan bijvoorbeeld naam, adres, e-mailadres en telefoonnummer, maar ook aan foto's, filmmateriaal, IP-adressen of cijfers, toetsen en werkstukken.

De AVG besteedt extra aandacht aan bijzondere persoonsgegevens. Dit zijn vaak gevoelige gegevens zoals iemands ras of etnische afkomst, politieke voorkeur, godsdienst, geaardheid, genetische of biometrische gegevens of gezondheid. Deze gegevens worden vanwege de gevoeligheid extra beschermd. Het is verboden om bijzondere persoonsgegevens te verwerken (verzamelen, opslaan en gebruiken), tenzij er een wettelijke uitzondering is.

Op school verwerken we persoonsgegevens van leerlingen, ouders en medewerkers. Dat begint al bij het inschrijven van een leerling of het voeren van een sollicitatiegesprek. Ook werkt de school met digitale systemen zoals toetsingsprogramma's en leerlingvolgsystemen en we maken gebruik van sociale media en apps. Soms delen we gegevens met derden, bijvoorbeeld met de overheid voor de bekostiging van het onderwijs, of met een extern bureau dat de salarissen verwerkt. Om dit veilig en verantwoord te doen, hebben we duidelijke afspraken die schriftelijk zijn vastgelegd in het privacyreglement.

**GA NAAR HET
PRIVACYREGLEMENT**



Veilig omgaan met persoonsgegevens?

Dat doe je zo!
Aan het gebruik van ICT- en bedrijfsmiddelen zoals een laptop of een werktelefoon zijn risico's verbonden, ook bij de bescherming van persoonsgegevens. Daarom zijn er afspraken gemaakt over het gebruik van deze middelen, die zijn vastgelegd in de Gedragscode ICT.

Op de volgende pagina een korte samenvatting van de afspraken in de Gedragscode:

**GA NAAR
GEDRAGSCODE ICT**



Samenvatting van de Gedragscode:

WAAR EN HOE BEWAAR IK PERSOONSGEGEVENS?



Bewaar gegevens digitaal
Bewaar persoonsgegevens zoveel mogelijk digitaal op de afgesproken (veilige) bewaarplaatsen.



Werk zorgvuldig en professioneel
Moet je gegevens over een persoon vastleggen? Zorg dan voor een zorgvuldige en professionele omschrijving.



Gebruik een veilige computer
Gebruik voor de verwerking van leerlinggegevens bij voorkeur een computer van school. Kan dat niet en moet je toch vanaf een privé computer werken? Zorg er dan voor dat deze goed beveiligd is.



Deel niet zomaar persoonsgegevens
Vraagt iemand jou om persoonsgegevens van een ander? Ga dan eerst na of dit nodig is en welke afspraken hierover binnen je school gemaakt zijn.

HOE EN WAT COMMUNICEER IK ONLINE?



Foto- en filmopnames delen
Wil je foto's of video's waarop leerlingen of collega's te zien zijn delen via bijvoorbeeld social media of de website? Controleer dan eerst of hiervoor toestemming is gegeven, schriftelijk dan wel online. Zo niet, dan mag je die foto's of video's niet delen.



Mail beveiligd
Het is veiliger om een link naar documenten te delen dan om deze als bijlage te versturen via e-mail. Maak voor gevoelige en bijzondere persoonsgegevens gebruik van een oplossing voor beveiligd mailen.



Pas op voor phishing en spoofing
Klik alleen op linkjes en open alleen bijlagen in e-mails van betrouwbare afzenders. Vul nooit je inloggegevens in op een website die je normaal hiervoor niet gebruikt en geef deze ook niet desgevraagd door aan iemand.



Gebruik BCC
Stuur je een bericht naar een (grote) groep mensen, die niet allemaal van je eigen organisatie zijn? Zet de e-mailadressen dan altijd in de BCC-regel.

HOE HOUD IK ONBEVOEGDEN OP AFSTAND?



Beveilig je computer en werkomgeving
Vergrendel je computer of meld je af als je je werkplek verlaat. Zorg ervoor dat er op je bureau en bij de printer geen gevoelige informatie ligt. En bewaar laptops of tablets op een veilige plek.



Pas op met meekijkers en -luisteraars
Zet je digibord op freeze als je wachtwoorden intoetst of persoonsgegevens in beeld staan. En zorg dat niemand meekijkt als jij je wachtwoord intoetst of meeluistert bij vertrouwelijke (telefonische) gesprekken.



Kies een sterk wachtwoord
Laat je wachtwoorden van digitale (administratie) systemen met persoonsgegevens niet onthouden door je internetbrowser. Kies een sterk wachtwoord, schrijf het niet op en deel het niet met collega's of anderen.



Gaat het mis? Meld het meteen!
Als je persoonsgegevens kwijt raakt, onbevoegden er toegang tot hebben gekregen, of als je gegevens niet meer toegankelijk zijn, meld dit dan meteen bij je leidinggevende. Het kan een datalek zijn.

Top 10 datalekken

En tips om deze te voorkomen!

Op school werk je dagelijks met persoonsgegevens. Daar gaan we vanzelfsprekend zorgvuldig mee om, zodat deze niet in verkeerde handen vallen. Niet alleen omdat de AVG dit voorschrijft, maar ook omdat het gaat om de bescherming van de privacy van leerlingen en medewerkers. Wanneer er toch iets fout gaat, dan kan er sprake zijn van een datalek. Hoe vervelend ook, weet wel dat het iedereen kan overkomen.

We spreken van een datalek of privacylek wanneer persoonsgegevens toegankelijk worden voor derden die over die gegevens geen beschikking zouden mogen hebben. Ook is er sprake van een datalek wanneer per

soonsgegevens verloren zijn geraakt en er geen back-up beschikbaar is. Het is belangrijk om een mogelijk datalek altijd direct te melden aan de privacy officer privacy@sanctamaria.nl, óók wanneer je twijfelt. Soms moet een datalek gemeld worden bij de Autoriteit Persoonsgegevens. Dat moet wettelijk binnen 72 uur gebeuren, dus het is belangrijk dat (mogelijke) datalekken snel worden gemeld.

Voorkomen is beter dan genezen, daarom staan hieronder de meest voorkomende datalekken in het onderwijs en wat jij kunt doen om deze te vermijden.

Top 10

1

Verkeerde persoon gemaild
Wees extra zorgvuldig bij het versturen van mails met persoonsgegevens en controleer altijd het mailadres voordat je op verzenden klikt.

2

Verkeerde bijlage gemaild
Verstuur geen bijlagen met gevoelige informatie per mail. Stuur een versleutelde mail of een link. Stuur de code om de mail of link te openen bij voorkeur per SMS.

3

Laptop gestolen/gehackt
Sla bestanden op in de beveiligde cloud-omgeving van de school. Werk je toch lokaal, zorg dan dat je harde schijf is versleuteld en je een backup hebt.

4

CC i.p.v. BCC gebruikt
Zet de mailadressen in de BCC regel wanneer je grote groepen ontvangers moet mailen. Berichten aan ouders of leerlingen stuur je het beste via het schoolportaal.

5

Meekijkers op je scherm
Vergrendel je beeldscherm, wanneer je wegloopt van je werkplek. Laat je browser geen wachtwoorden onthouden. Schrijf geen wachtwoorden op!

6

Smartphone onbeveiligd
Beveilig je mobiele telefoon met een goed wachtwoord, wanneer je mail of schoolapps erop hebt staan! Zo is deze beter beschermd bij diefstal.

7

Phishingmail
Controleer een link door met je muis over de link te bewegen. Je ziet dan waar de link naartoe leidt. Open geen bijlagen van afzenders die je niet kent.

8

Misbruik beeldmateriaal
Leg toestemming aantoonbaar vast en publiceer geen beeldmateriaal zonder toestemming van de betrokken personen.

9

Te veel inzage(rechten)
Ga na of je meer gegevens kunt zien of bewerken dan je nodig hebt voor je werk. Meld dit indien dit het geval is.

10

Rondslingerende documenten
Laat documenten met persoonsgegevens niet onbeheerd achter (denk hierbij aan printer, postvak, klassenmap, USB-stick)!

10

Leerlingdossier

In het leerlingendossier slaan we alle informatie op die van belang is bij het onderwijsproces. Dit kunnen adresgegevens, financiële gegevens of gegevens over aan- en afwezigheid zijn, maar ook medische gegevens mits deze relevant zijn voor het onderwijsproces of gegevens die betrekking hebben op incidenten.

Toegang tot het leerlingdossier hebben uitsluitend medewerkers van Sancta die hiervoor aangewezen zijn, zoals de schoolleiding, teamleiders, docenten (gedurende de periode dat ze de betreffende leerling lesgeven), conciërges en medewerkers van de trajectbegeleiding. Bovendien mogen deze medewerkers gegevens in het dossier alleen raadplegen of aanvullen als dit relevant is bij hun werk. Wie toegang heeft tot welke programma's en documenten is vastgelegd in een overzicht genaamd 'autorisatiematrix'.

Op grond van de AVG hebben ouder(s)/verzorger(s) het recht om het dossier van hun kind in te zien of een ko-

pie hiervan te ontvangen als het kind jonger dan 16 jaar is. Voor leerlingen van 16 jaar en ouder geldt echter dat niet hun ouder(s)/verzorger(s) maar zichzelf dit recht hebben. Inzage of verstrekken van een kopie vindt uitsluitend plaats zonder afbreuk te doen aan de rechten en vrijheden van anderen, dit ter beoordeling van de privacy officer.

Communicatie over leerlingen

Communicatie over leerlingen verloopt zoveel als mogelijk via het logboek in Magister. Met name indien de communicatie bijzondere persoonsgegevens bevat (informatie over ras of etnische afkomst, politieke voorkeur, godsdienst, geaardheid, genetische of biometrische gegevens of gezondheid) is het van belang te kiezen voor Magister als het meest veilige communicatiemiddel.

Dossier medewerkers

Het hebben van een personeelsdossier is wettelijk verplicht. In dit dossier zit bijvoorbeeld de getekende arbeidsovereenkomst, verslagen van functioneringsgesprekken en beoordelingsgesprekken, informatie over ziekteverzuim en salariering. Wie er toegang heeft tot het personeelsdossier is eveneens vastgelegd in de 'autorisatiematrix'. Een medewerker heeft recht op inzage en mag een kopie van zijn personeelsdossier opvragen.

Gegevens delen met derden?

Wil je gegevens uitwisselen met een externe organisatie? Let dan altijd goed op en houd rekening met de privacyregels. In bepaalde gevallen heb je toestemming nodig, maar niet altijd. Met sommige organisaties mogen (of moeten) we wél gegevens uitwisselen zonder formele toestemming. Zo is het bij wet geregeld dat er meestal geen toestemming nodig is voor het delen van persoonsgegevens met de Inspectie van het Onderwijs, Veilig Thuis, het Samenwerkingsverband, de overdracht po-vo en de leerplichtambtenaar, salariering met het salarisverwerkingsbureau etc.

Wil je gegevens uitwisselen met externen, zoals een logopedist, een arbo- of schoolarts, jeugdzorg of een schoolbegeleidingsdienst? Dan is het wel nodig om toestemming te vragen van ouder(s) of verzorger(s), aan de leerling of aan de medewerker. Zorg ervoor dat je de toestemming registreert (bewaard in Magister of het personeelsdossier) en houdt daarbij - afhankelijk van de leeftijd van de leerling - ook rekening met de verdeling van het ouderlijk gezag. Overleg laagdrempelig met de privacy officer.





Bewaartermijnen op school

Opgeruimd staat netjes!

Scholen zijn verplicht om bepaalde informatie gedurende een vastgestelde tijd te bewaren. De wijze waarop en de termijnen staan onder andere beschreven in de Archiefwet en in de AVG. Op school zijn deze wetten vertaald naar een procedure met bewaartermijnen en verantwoordelijken. Voor sommige persoonsgegevens zijn wettelijke bewaartermijnen vastgesteld.

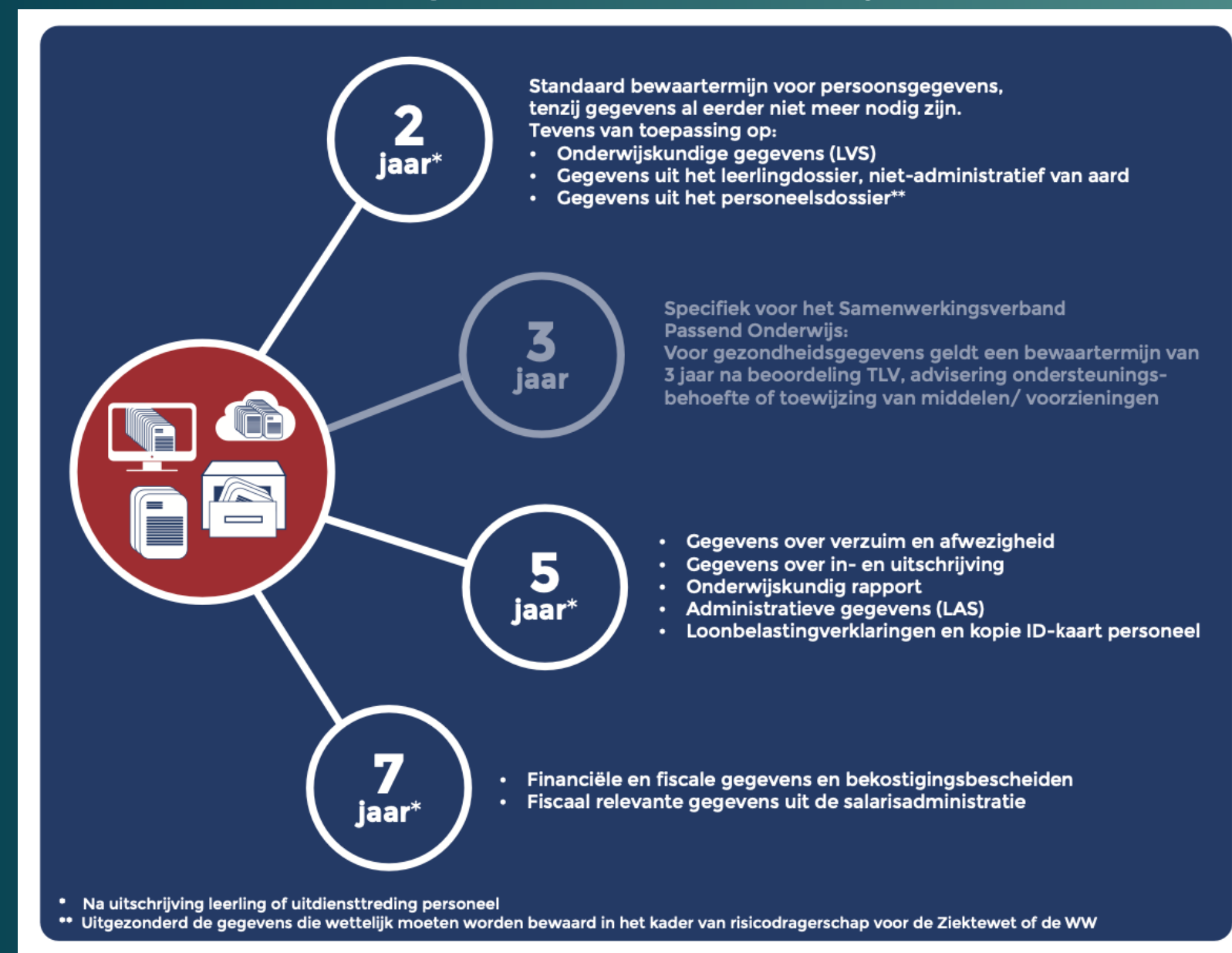
Wanneer opslag van persoonsgegevens niet meer noodzakelijk is, moeten ze worden gewist of vernietigd. Het is belangrijk te weten dat documenten

met persoonsgegevens niet zomaar in een prullenbak mogen worden weggegooid. Zij moeten op een juiste manier vernietigd worden. Maak gebruik van de papierversnipperaars of gooi de documenten weg in de speciale gesloten archiefbakken die op school aanwezig zijn. Het gaat hierbij ook om toetsen, klassenlijsten, foto's etc.

Heb je hulp nodig bij het bepalen van bewaartermijnen? Overleg laagdrempelig met de privacy officier, raadpleeg deze infographic of het uitgebreide bewaar en vernietigingsbeleid.



Samenvatting bewaartermijnen:



**GA NAAR BEWAAR EN
VERNIETIGINGSBELEID**



Phishing

Hoe vis je ze eruit?

Phishing is een ernstige vorm van computercriminaliteit. Door gebruik van valse WhatsApp-berichten, e-mails of sms'jes, word je naar een nagebootste website gelokt van bijvoorbeeld je bank of wordt er ongemerkt software op je computer geïnstalleerd. Hiermee krijgen criminelen toegang tot je bankrekening, bestanden op je computer of je webcam. Dit kan leiden tot bankroof, datalekken of situaties waarin je een geldbedrag moet betalen om weer bij je bestanden te komen. Het is dus belangrijk om te weten hoe je phishing kunt herkennen en deze vorm van computerinbraak kunt voorkomen.

Phishing: Sla ze aan de haak

WEL DOEN

☐ Bericht markeren als SPAM

☐ Melden bij Privacy Officer

☐ Collega's informeren

NIET DOEN

☐ Op links klikken

☐ E-mail doorsturen

☐ Gegevens invoeren

LET OP: je bank, verzekering of andere officiële instanties vragen nooit om je inloggegevens of andere persoonlijke codes.

Phishing: Vis ze eruit

Phishingberichten...

... komen meestal onverwacht en zonder reden.

... hebben een dwingende taal of willen je nieuwsgierig maken.

... bevatten steeds minder taalfouten en zien er steeds professioneler uit.

... gebruiken je e-mailadres als aanspreektitel of iets anders onpersoonlijks.

... vragen je altijd om door te klikken.

... hebben een onbekende afzender, een afzender die lijkt op een bekende afzender, een dubieus e-mailadres of bijlage.

Onderzoek

Steeds vaker wordt gebruik gemaakt van (online) enquêtes. Alle enquêtes die namens Sancta of in opdracht van Sancta of ten behoeve van het onderwijsproces (PWS of Quest bijvoorbeeld) worden afgenomen zijn anoniem, er wordt niet gevraagd naar persoonsgegevens. Indien het voor het onderzoek van belang is wel te vragen naar persoonsgegevens, dan dient er een privacyverklaring te worden toegevoegd die is goedgekeurd door de privacy officer. In de privacyverklaring moet duidelijk staan hoe er wordt omgegaan met de gegevens die verzameld worden. Deze privacyverklaring moet dan ook nageleefd worden. Een uitzondering betreft bijzondere persoonsgegevens, hier mag nooit in een enquête naar gevraagd worden. Bij online enquêtes mag daarnaast alleen gebruik gemaakt worden van Microsoft Forms, het gebruik van Google Forms of andere aanbieders is niet toegestaan.

Extern onderzoek

Scholen worden regelmatig benaderd om deel te nemen aan een onderzoek en daarvoor persoonsgegevens van leerlingen of medewerkers aan te leveren. Dit betekent dat deze gegevens worden uitgewisseld met een andere organisatie, die het verwerkt voor dit onderzoek. Wanneer kan de school wel en wanneer niet deelnemen aan zulk extern onderzoek? Waar moet de school rekening mee houden? Wat moet je controleren en regelen voordat de data worden gedeeld? Voldoet het onderzoek aan de basisprincipes van de AVG? Onderstaand stroomschema geeft hier inzicht in.

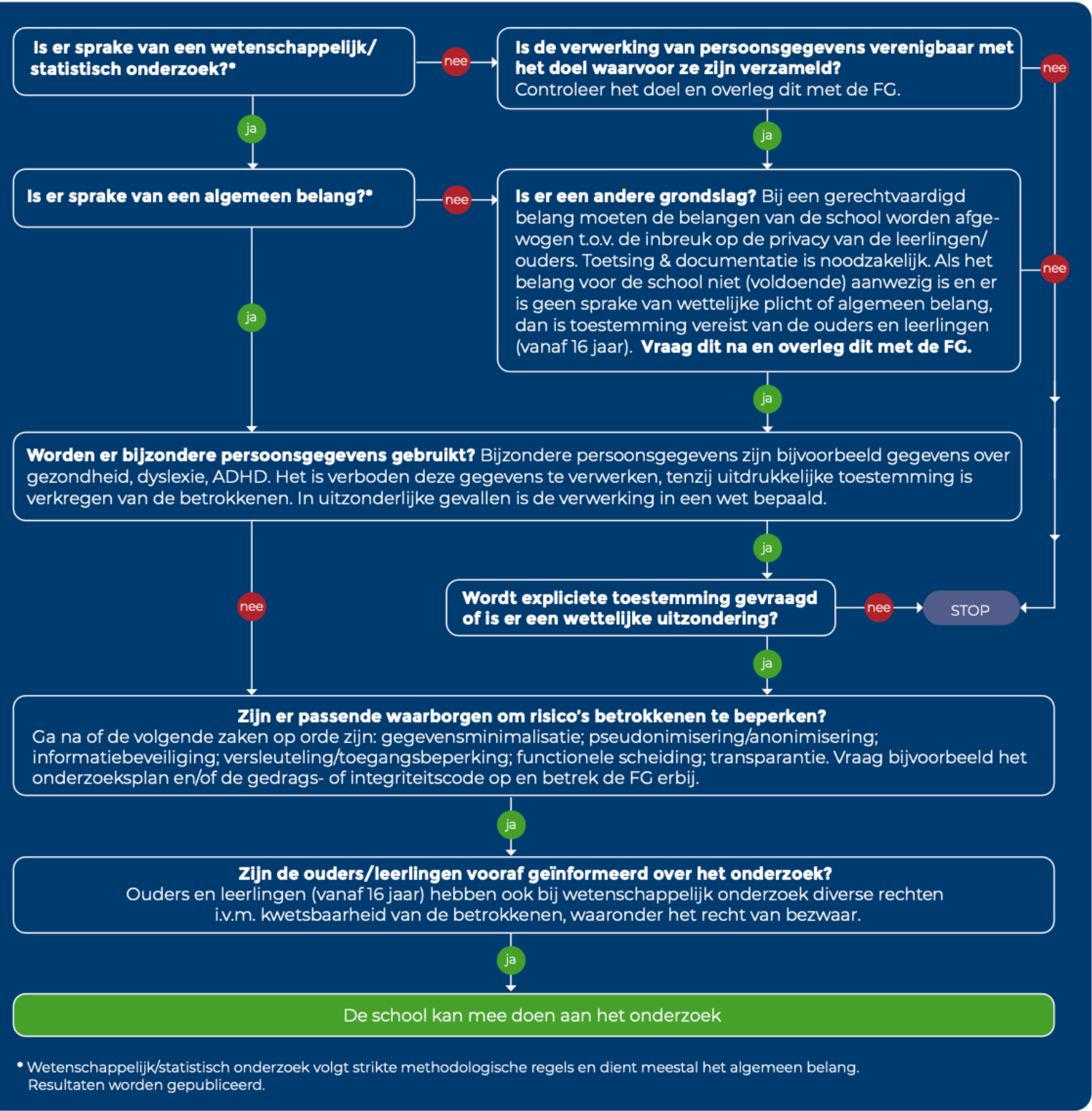


Foto en Film op school

Waar moet ik dan aan denken?
Omdat het maken en publiceren van foto en filmmateriaal niet onder de onderwijstaak van school valt, is er altijd schriftelijke toestemming nodig: leerlingen van 16 jaar en ouder geven zelf toestemming en in andere gevallen de ouders of wettelijk vertegenwoordigers. In Magister staat aangegeven of die toestemming is verkregen en jaarlijks krijgen ouders en leerlingen het verzoek deze gegevens te controleren en opnieuw toestemming te geven. Controleer Magister vóórdat je een foto of filmpje maakt. Maak je beeldmateriaal met een eigen apparaat? Vergeet niet om dat weer uit je persoonlijke fotobibliotheek te verwijderen. De beelden zijn tijdens het werk gemaakt, ten behoeve van het werk en mogen nooit verspreid worden via privé (sociale media) kanalen.

Voor het gebruik van pasfoto's in het leerlingvolgsysteem is geen toestemming nodig. Dat gebruik ter identificatie is immers rechtstreeks verbonden aan de onderwijstaak van de school. Op pasfoto's dienen leerlingen goed herkenbaar in beeld te zijn, niet verkleed of voorwerpen dragend die identificatie kunnen bemerkeren, zoals een pet of zonnebril.

Leerlingen onderling maken ook vaak filmpjes en foto's. Regels hierover zijn vastgelegd in het sociale mediabeleid.

GA NAAR HET SOCIALE MEDIABELEID.



Cameratoezicht

Lyceum Sancta Maria maakt gebruik van camera-toezicht. Wij gebruiken cameratoezicht uitsluitend voor de volgende doeleinden:

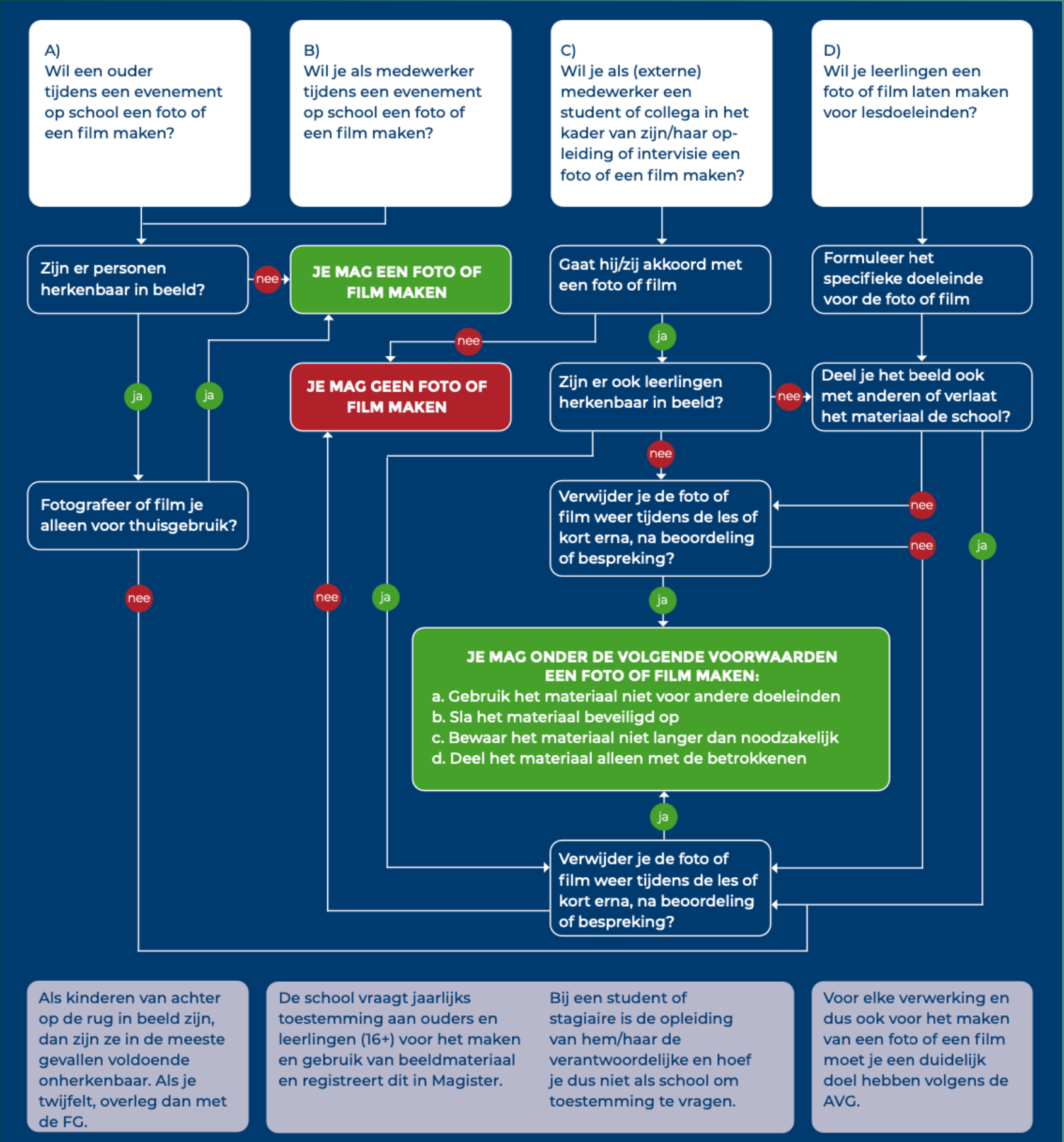
- Bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers.
- Beveiliging van toegang tot gebouwen en terreinen.
- Bewaking van zaken die zich in gebouwen of op terreinen van de school bevinden.
- Vastleggen van incidenten.

Alleen aangewezen medewerkers mogen camerabeelden bekijken, volgens een afgesproken protocol. De camera's hangen zichtbaar in en rond de school: er wordt in principe geen gebruik gemaakt van verborgen camera's en niet gefilmd op privacy-gevoelige plekken zoals kleedkamers. Het bekijken van beelden wordt uitsluitend gedaan indien hier aanleiding toe is en indien er wordt voldaan aan bovengenoemde doeleinden. Ze worden incidentgericht bekeken.

Ondanks het feit dat de camera's continue registreren, wordt er niet steevast gemonitord. Het is leerlingen/ouders of niet-aangewezen personen niet toegestaan om mee te kijken bij het monitoren. Ouders, leerlingen, medewerkers en bezoekers kunnen onder bepaalde voorwaarden echter wel camerabeelden opvragen: deze aanvraag verloopt via de privacy officer. De politie kan camerabeelden uitsluitend verkrijgen na het overleggen van een vordering met de juiste grondslag. Zonder correcte vordering worden beelden niet overhandigd. De mogelijkheid om 'daders' van misstanden op een andere wijze op te sporen, bijvoorbeeld door het uitlezen van IP-adressen, is niet toegestaan.



**GA NAAR HET
PROTOCOL
CAMERATOEZICHT.**

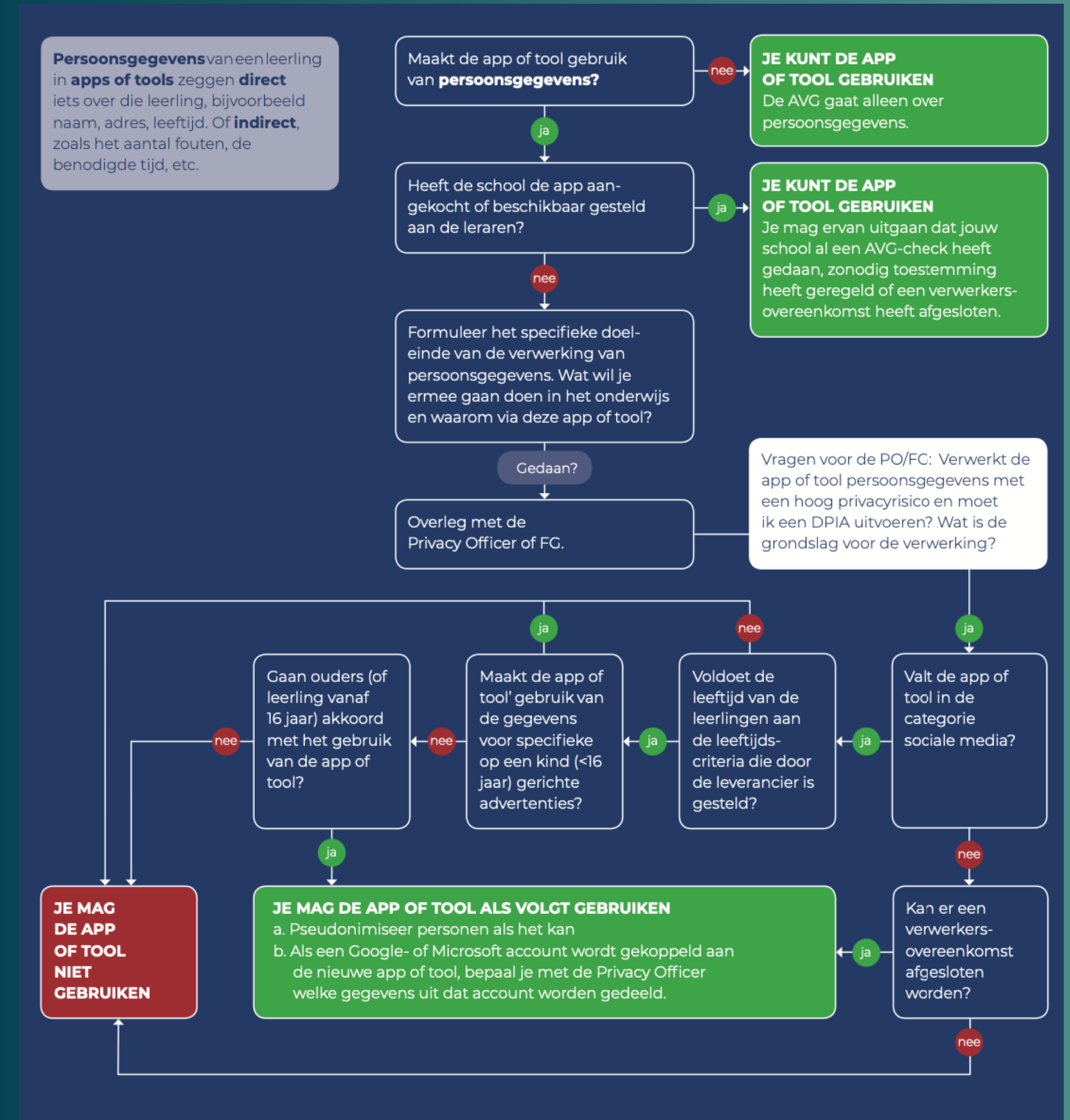




Apps en tools op school

Waar moet ik aan denken?

Wil je een (socialmedia-app) gaan gebruiken. Dan zijn er een aantal zaken waar je rekening mee moet houden. De flowchart op de volgende pagina geeft inzicht hier in.





www.sanctamaria.nl