INf2.8.2

Werkveld	Datum	Instemming/Advies GMR	Vastgesteld CvB
ICT	22 mei 2023	A - 4 oktober 2023	16 oktober 2023

2.8.2 | Informatiebeveiliging en privacy

Handboek

Inhoudsopgave

1. Toegang ParnasSys

Alleen leerkrachten en administratief medewerkers van Aves krijgen, door HRM, toegang tot ParnasSys voor de locatie waar zij op dat moment werkzaam zijn. Alle gebruikers van ParnasSys maken gebruik van de twee-staps-verificatie. Alle gebruikers van ParnasSys krijgen alleen toegang tot de groepen die noodzakelijk zijn voor het goed uitvoeren van hun taak.

Er is een uitzondering voor WPO studenten en trainees. Zij krijgen tijdens de stageperiode toegang tot ParnasSys, met een beperkt account. Zij krijgen alleen toegang tot de eigen groep met gebruik van de twee-staps-verificatie.
Onderwijsondersteuners en externe partijen zoals een samenwerkingsverband, logopedie etc. krijgen geen toegang tot ParnasSys. In sommige gevallen betekent dit dat uitwisseling van gegevens handmatig gebeurt.

Aves houdt bij het gebruik van ParnasSys de vijf basisregels van de privacywetgeving in acht.

1.1 Doelbepaling en doelbinding

Medewerkers met een ParnasSys account hebben toegang tot leerlinggegevens. Dit zijn gegevens van leerlingen die in de **eigen** groep zitten en noodzakelijk zijn om goed onderwijs te kunnen bieden. Een uitzondering hierop zijn leerkrachten die een extra ondersteunende rol hebben binnen de school. De directeur bepaalt en stelt de uitbreiding op toegang tot leerling dossiers in.

1.1 Grondslag

De verwerking van de gegevens van leerlingen is noodzakelijk om tot een goede onderwijsondersteuning te komen. Hierbij is de expertise van het onderwijsteam en ouders samen nodig om tot goed onderwijs te komen.

1.2 Dataminimalisatie

- Directeuren, ib'ers en leerkrachten werkzaam voor Aves krijgen alleen toestemming tot de leerling gegevens van de schoollocatie waar zij werkzaam zijn.
- Leerkrachten en onderwijsondersteuners krijgen alleen toegang tot leerlinggegevens van de groep waar zij onderwijs verzorgen.

1.3 Transparantie

In de schoolgids staat vermeld dat:

- De school gebruik maakt van ParnasSys en dat er met bepaalde partijen informatie wordt uitgewisseld met een duidelijk onderwijsdoel.
- Iedere ouder heeft recht op inzage in het leerlingdossier van zijn of haar kind.

1.4 Data – integriteit

De persoonsgegevens worden door de directeur van de locatie ingevoerd en actueel gehouden. In sommige gevallen gebeurt dit via het ouderportaal. De directeur is verantwoordelijk voor het toegangsbeheer binnen de eigen locatie.

1.5 Controle

ParnasSys voldoet aan de eisen van de AVG. De toegang in ParnasSys wordt geregistreerd en is te controleren via Beheer – Gegevenstoegang. Door PZ wordt 2 maal per jaar een controle uitgevoerd om te zien of er ongeoorloofd toegang is in ParnasSys. Dit wordt gerapporteerd aan de manager ibp.

1.6 Accountbeheer

Alle ParnasSys accounts zijn georganiseerd via de bovenschoolse module. De medewerker krijgen van PZ een bestuursaanstelling en toegangsrechten op de school waar de medewerker komt te werken. De applicatiebeheerder (directeur) van de school kan daarna de rechten aanpassen en de medewerker koppelen aan de groep.

1.7 Twee-staps-verificatie

Aves erkent het belang van een goede beveiliging van privacygevoelige informatie. Dit betekent dat een ParnasSys account met een sterk wachtwoord door de gebruiker is beveiligd. Alle medewerkers van Aves maken gebruik van de twee-staps-verificatie.

1.8 Leerkrachten app

Wordt er gebruik gemaakt van de leerkrachten app van ParnasSys, Parro of een andere app waar privacygevoelige informatie zichtbaar is, dan verwacht Aves van de medewerker dat het gebruikte apparaat goed beveiligd is met een pincode, sterk wachtwoord, vingerafdruk of irisscan. Bij verlies of diefstal van het apparaat, welke voorzien is van deze informatie dient aangifte gedaan te

worden en moet er binnen 24 uur melding gemaakt worden bij de manager ibp via privacy@aves.nl. Het protocol datalek zal in werking worden gezet.

1.9 Inhoud

Alle Aves scholen maken gebruik van ParnasSys als Leerling Administratie Systeem (LAS). Hierin worden persoonsgegevens, leerling resultaten, observaties, verslagen en eventuele onderzoeken opgeslagen. Hieronder een overzicht;

- gegevens over in- en uitschrijving
- gegevens over afwezigheid
- adresgegevens
- gegevens die nodig zijn om te berekenen hoeveel geld de school krijgt
- het onderwijskundig rapport
- gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen
- gegevens over de vorderingen en de resultaten van de leerling
- verslagen van gesprekken met de ouders
- de resultaten van eventueel onderzoeken.

1.10 Bewaartermijnen

Er zijn vastgestelde bewaartermijnen voor leerling dossiers. In de bijlage een overzicht van deze termijnen. Adresgegevens mogen wel bewaard worden voor onbepaalde tijd.
De directeur is verantwoordelijk voor het verwijderen van leerling dossiers die buiten het vastgestelde termijn vallen.

1.11 Controle

PZ is verantwoordelijk voor mutaties in ParnasSys. Op 2 momenten in het jaar wordt er een controle gedaan door PZ of de teams nog actueel zijn. Het resultaat wordt met de manager IBP besproken.

2. Studenten en onderwijsondersteuners

WPO studenten, trainees en onderwijsondersteuners krijgen:

- Een Microsoft365 account. PZ is verantwoordelijk voor het aanmaken van een PNIL (persoon niet in loondienst) account in Visma.
- Wpo studenten, trainees en onderwijsondersteuners ontvangen een ParnasSys account en worden gekoppeld aan de school. Toegang tot de groep is de verantwoordelijkheid van de directeur.

Voor Wpo studenten, trainees en onderwijsondersteuners geldt een geheimhoudingsverklaring als het gaat om privacygevoelige informatie. Dit is via de aanstelling of via of via de “Handreiking stagiaires” geregeld door PZ of de betreffende directeur.

3. Tienercollege

Het Tienercollege is in ontwikkeling samen met het Emelwerda college. Beide partijen hebben een gezamenlijke verantwoordelijkheid om de privacy te waarborgen. Hiervoor is de structuur van het Tienercollege in kaart gebracht. Er kwamen een aantal verbeterpunten naar voren:

1. Een geheimhoudingsverklaring is noodzakelijk voor de betrokken docenten en leerkrachten.
2. Verwerkersovereenkomsten voor beide onderwijsorganisaties moeten worden afgesloten met de softwareleveranciers.
3. Privacy moet op de website van het Tienercollege een plaats krijgen.
4. Bij het maken van klassenfoto’s zal een verwerkersovereenkomst noodzakelijk zijn.
5. De stuurgroep wordt op de hoogte gehouden over de verbeterpunten.

4. Datalekken

Alle mogelijke vormen van datalekken dienen binnen 72 uur gemeld te worden via privacy@aves.nl. De manager ibp maakt een melding bij de Autoriteit Persoonsgegevens. In dit hoofdstuk staat beschreven hoe Aves omgaat met mogelijke datalekken.

Gebruikte termen:

- Beveiligingsincident; een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- Informatievoorziening; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- Datalek; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- Betrokkene; de persoon van wie de persoonsgegevens zijn gelekt.

4.1 Werkwijze

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1 Ontdekker (medewerker); degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2 Meldpunt (manager ibp); een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt. Bij Aves worden alle beveiligingsincidenten gemeld bij de manager ibp; privacy@aves.nl
3 Melder (manager ibp); degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4 Technicus (netwerkbeheerder, uitgever of ict-coördinator); degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

4.2 Ontdekken

De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt dit binnen 48 uur bij de manager ibp via privacy@aves.nl. De ontdekker zal gevraagd worden een incidentenformulier in te vullen (bijlage 3). Deze zal door de manager ibp verstrekt worden.

4.3 Inventariseren

De manager ibp bepaalt of er voldoende informatie over het beveiligingsincident bekend is en stelt waar nodig aanvullende vragen aan de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd in het document Register beveiligingsincidenten (dit document zal op het bestuursportaal komen te staan):

- Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
- Datum/periode van het beveiligingsincident
- Aard van het beveiligingsincident
- Wanneer van toepassing (bij een datalek):
- Omschrijving van de groep betrokkenen
- Aantal betrokkenen
- Type persoonsgegevens in kwestie
- Worden de gegevens binnen een keten gedeeld

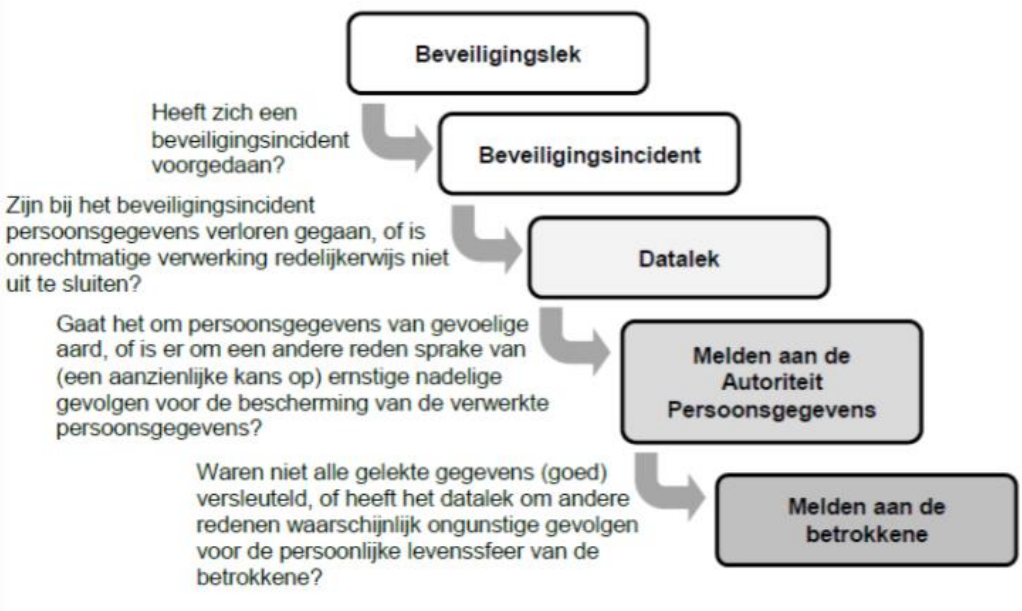
4.4 Beoordelen

Wanneer de manager ibp voldoende informatie heeft verzameld, zal hij indien nodig in samenspraak met de Voorzitter van het college van bestuur beoordelen of er sprake is van een ‘meldingsplicht datalek’. Bij de beoordeling of er sprake is van een ‘meldingsplichtig datalek’, wordt rekening gehouden met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, móet er gemeld worden.
Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens “gevoelig” zijn, zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de

betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

De volgende informatie wordt vastgelegd:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?



4.5 Repareren

De Technicus wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. Hierbij wordt vastgelegd welke technische en organisatorische maatregelen genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.

4.6 Melden

Als de conclusie is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de manager ibp dit in samenspraak met het college van bestuur binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0 .

4.7 Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de manager ibp (Register beveiligingsincidenten). De manager ibp geeft terugkoppeling van de genomen maatregelen aan de Ontdekker.

4.8 Informeren betrokkene: leerling en/of zijn ouders

Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers en of ouders van de betrokken leerlingen. In principe kan ervan uit worden gegaan dat het lekken van informatie van gevoelige aard gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat níet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

4.9 Monitoring

De manager ibp informeert het cvb 1 keer per jaar over eventuele beveiligingsincidenten en datalekken. Hierbij wordt vooral gekeken of er structurele aanpassingen noodzakelijk zijn om deze incidenten te voorkomen.

4.10 Communicatie

Alle medewerkers worden door de directeur en of de ict'er van de school geïnformeerd over de meldplicht bij datalekken. Hierbij wordt vooral ingegaan op de volgende onderwerpen;

- Vermoeden van onterecht uitwisselen van leerling gegevens (bijvoorbeeld het ontvangen van aanbiedingen van commerciële bedrijven die rechtstreeks op leerresultaten van een groep of individuele leerlingen terug te voeren zijn.)
- Datalek door verlies/diefstal van apparatuur en/of inloggegevens. We gebruiken steeds meer apparatuur bij ons werk, denk daarbij aan je tablet of je smartphone. Al deze apparatuur kan gegevens bevatten, die niet toegankelijk mogen zijn voor anderen (ParnasSys leerkrachten app, informatie op je tablet). Diefstal of verlies van deze apparatuur kan leiden tot een datalek, als de apparatuur of de apps niet goed beveiligd zijn.
- Clean desk policy & wachtwoordbeleid. Wachtwoorden die toegang verschaffen tot applicaties waarin persoonsgegevens zijn opgeslagen mogen niet opgeschreven worden. Werknemers zorgen ervoor dat ze geen privacygevoelige informatie open laten staan op onbeheerde devices. Zet je pc op slot met Windows toets + L, gebruik een code voor je telefoon. Digitale

bestanden met persoonsgegevens worden opgeslagen op daarvoor bestemde locaties (SharePoint, OneDrive of ParnasSys). Memory sticks worden niet gebruikt.
- Toestemming voor gebruik software aanvragen. Om te voorkomen dat er softwareprogramma's gebruikt worden waarbij persoonsgegevens worden verstrekt aan leveranciers waar geen verwerkersovereenkomst mee is afgesloten, mogen alleen programma's gebruikt worden waarmee een verwerkersovereenkomst is afgesloten. De lijst met leveranciers en programma's is te vinden in hoofdstuk 5. Als een school een nieuw programma wil gebruiken die niet in de lijst voor komt, moet contact opgenomen worden met de manager ibp.
- Veilig mailverkeer. Het versturen van persoonsgegevens via e-mail is niet toegestaan.
    - Directeuren en ib'ers hebben een Zivver account waarmee beveiligd informatie verstuurd kan worden.
    - Beveiligde documenten mogen als bijlage, afzonderlijk van het wachtwoord, gedeeld worden vanuit de Microsoft365 omgeving.
    - Wachtwoorden die via de email verstuurd worden dienen door de betrokkenen na verwerking verwijderd te worden.

Via de website van Aves en de email zullen medewerkers en ouders geïnformeerd worden over eventuele incidenten. Bij geïsoleerde incidenten (op schoolniveau welke geen invloed hebben op de organisatie) zal de directeur in overleg met de manager ibp en het cvb de betrokken per email inlichten en dit kenbaar maken op de website van de school.

5. Afspraken met leveranciers

Aves maakt als schoolbestuur en verantwoordelijke voor de persoonsgegevens afspraken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Afgesproken wordt:
- Hoe informeer je elkaar over datalekken.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatiegegevens de bewerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding (maak afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de bewerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

De schriftelijke afspraken die Aves maakt met haar verwerker(s) over datalekken worden vastgelegd in een verwerkersovereenkomst.

5.1 Overzicht verwerkersovereenkomsten

	Bewerker
10-9-2018	Entree Federatie
10-9-2018	Nummervoorziening
5-7-2018	Drempelonderzoek
4-6-2018	Digitaal eindtoets
15-5-2020	WIS Collect
26-6-2018	IEP eindtoets
26-4-2018	Cito LOVS
14-12-2018	Dedicon
20-1-2020	Eindtoets (Tienercollege)
26-9-2018	Foto Koch
3-6-2019	Gynzy & Gynzy Kids
2-10-2019	Advies
22-11-2019	KanVAS
18-6-2018	Kindkans
13-10-2021	MTO
4-6-2018	Klasseplan
8-6-2018	Konnect
7-7-2018	LOGO-digitaal
8-10-2021	Schoolfotografie
31-5-2018	MijnOnderwijsportaal, Visma, Tobias, Spend Cloud
5-6-2018	Onlineklas
26-11-2018	Overstapservice onderwijs
18-5-2018	ParnasSys
15-5-2018	Prowise Presenter
12-6-2018	SCOL
3-9-2018	Schoolwise
20-6-2018	SchouderCom
26-11-2018	Snappet
15-4-2020	Social Schools
15-6-2018	Basispoort
3-7-2018	MijnRapportfolio

15-5-2018	Divers
30-10-2019	Vensters PO
11-10-2021	InvalPool
25-2-2021	Schoolsupport
19-8-2021	Bouw!
22-3-2021	Weektaak.com
26-6-2018	WIS Talent Manager
11-6-2018	Jamf
26-11-2018	Digitaal Handelingsprotocol Begaafdheid
24-11-2021	RTTI-Online
25-10-2021	Zivver
15-1-2018	Malmberg
13-1-2022	Easyrapport
15-9-2022	Ziber Education
4-11-2022	MQ Scan
24-10-2022	Stimuliz

Deze lijst zal door de manager ibp continu bijgewerkt worden, neem hiervoor contact op met de manager ibp

6. Toegang en wachtwoordbeleid

Wie toegang heeft tot de verschillende systemen met informatie wordt geregeld via het toegangsbeleid (zie bijlage 5). De toegang geldt voor medewerkers die contractueel verbonden zijn aan Aves.

6.1 Uitzondering tijdens inwerkperiode

Er is een belangrijke uitzondering op het toegangsbeleid. In sommige situaties is het wenselijk dat een persoon voor of na de datum in dienst toegang heeft tot de systemen van Aves. Dit zorgt in de meeste gevallen voor een soepelere overgang bij bijvoorbeeld de aanstelling van een nieuwe directeur of ib'er.
Met toestemming van het bestuur, in overleg met de manager HRM en het ondertekenen van een geheimhoudingsverklaring is toegang tot de systemen van Aves mogelijk.

6.2 Het belang van correcte omgang met wachtwoorden

Wachtwoorden vormen een belangrijk aspect van de beveiliging van persoonlijke informatie over leerlingen, ouders en medewerkers van Aves (vallen onder AVG en worden vanaf nu "bijzondere gegevens" genoemd). Wachtwoorden zorgen ervoor dat onbevoegden geen toegang kunnen krijgen tot de bijzondere gegevens van leerlingen, ouders en medewerkers.
Alle medewerkers van Aves gebruiken een goed wachtwoord en zijn verantwoordelijk voor de geheimhouding van hun wachtwoorden en inloggegevens. (Dit is mogelijk door hun eigen wachtwoorden in een door henzelf beveiligd document op te slaan, deze gegevens worden daarna uit de emailomgeving verwijderd.)

6.3 Wachtwoorden

Wachtwoorden hebben een bepaalde sterkte nodig om het moeilijker te maken dat ze worden geraden. De sterkte van een wachtwoord wordt bepaald door de lengte, de complexiteit en de onvoorspelbaarheid. Zwakke wachtwoorden zijn vaak te kort, zijn een te eenvoudig woord of zijn een eenvoudige toets combinatie. Hierdoor zijn ze makkelijk te raden. Medewerkers van Aves gebruiken een sterk wachtwoord bij de verschillende programma's.
Aves hanteert de volgende definitie van een sterk wachtwoord:
Een sterk wachtwoord is een wachtwoord dat minimaal bestaat uit 8 tekens, minimaal 1 hoofdletter, 1 cijfer en 1 symbool (bijvoorbeeld: !,@,#,$,%)

De beheerder van de Micorsoft365 omgeving (Comlog) hanteert de volgende eisen voor de toegang tot de Microsoft365 omgeving:
1. Het wachtwoord moet minimaal 8 karakters bevatten.
2. Het wachtwoord mag geen delen van u naam of van de school bevatten.
3. Het wachtwoord moet minstens 1 hoofdletter hebben, minstens 1 cijfer hebben en er moet een speciale teken in zitten.

De medewerker van Aves is zelf verantwoordelijk voor het veilig bewaren van de wachtwoorden.

6.4 Twee-staps-verificatie Microsoft 365

Aves onderkent het belang van goede beveilig op systemen met privacygevoelige informatie. Om deze reden maakt Aves gebruik van de twee-factor-authenticatie. Voor het inloggen op de Microsoft Surface wordt Windows Hello gebruikt.

6.5 Bij verlies of diefstal van wachtwoorden

Als er een vermoeden bestaat van verlies of diefstal (al dan niet digitaal, bijvoorbeeld phishingmail) van wachtwoorden, is de gebruiker verplicht de wachtwoorden direct aan te passen en dit verlies te melden bij de directeur. De directeur zal contact opnemen met de manager ibp via privacy@aves.nl, welke een mededeling zal verspreiden om herhaling te voorkomen.

7. Expertisenetwerk

Iedere beeldcoach maakt gebruik van een externe harde schijf. Met de beeldcoaches zijn de volgende afspraken gemaakt;

- Papierendossiers worden niet gebruikt.
- Een beeldcoach vraagt toestemming aan de ouders als er sprake is van individuele begeleiding.
- Als er geen sprake is van individuele leerlingbegeleiding, maar van begeleiding van de leerkracht is toestemming van ouders niet noodzakelijk. Informeren is wel van belang.
- De school is verantwoordelijk voor het informeren van ouders.
- Harde schijf met beeldmateriaal is beveiligd via Bitlocker
- Beelden worden na het coaching traject verwijderd door de beeldcoach.
- Beelden worden niet gedeeld aan personen buiten het coaching traject.

Bovenstaande afspraken gelden ook voor andere specialisten (Hoogbegaafdheidspecialist, NT2, gedragsspecialist) in het Expertisenetwerk, als zij gebruik maken van beeldmateriaal.

8. Oudervereniging

De Oudervereniging zijn opgericht als een eigen rechtspersoon. Dit betekent dat zij zelfstandig functioneren. De Oudervereniging zijn juridisch zelf verantwoordelijk voor het naleven van de AVG.

Als de school NAW, telefoonnummer, emailadres en bankrekeningnummer deelt met de Oudervereniging, moet hiervoor toestemming gegeven worden door ouders. Dit kan in het inschrijfformulier worden opgenomen. Het is ook opgenomen in het document “Toestemming gegevensverwerking”

9. Overstapservice Onderwijs (OSO)

Aves maakt gebruik van ParnasSys als leerling administratiesysteem. In ParnasSys zit privacygevoelige informatie. Om de overstap van PO naar PO en PO naar VO soepel en vooral veilig te laten verlopen is de Overstapservice Onderwijs (OSO) ontwikkeld.
Aves is voor het gebruik van OSO gecertificeerd. Alle scholen maken voor de overdracht van PO naar VO en PO naar PO gebruik van OSO. Om dit mogelijk te maken zal er toestemming verleend moeten worden van de ouders van de betreffende leerling. Zij moeten inzage gehad hebben in het overstapdossier. Hiervoor dient door de ouder/verzorger altijd getekend te worden. Bij de overstap van PO naar VO zal dit gebeuren op het aanmeldformulier. Als een leerlingen wisselt van PO naar PO, dan zal de ouder/verzorger tekenen op een toestemmingsformulier waarmee ze toestemming geven voor de digitale overdracht van het overstapdossier.

10. Tablets

Doordat Aves tablets beschikbaar stelt aan zijn medewerkers is het belangrijk om afspraken te maken met betrekking tot het gebruik in verband met toegang tot “bijzondere gegevens”. Hiervoor is een gebruikersovereenkomst opgesteld. Deze wordt door de gebruiker ondertekend.

Aves geeft in vol vertrouwen de leerkrachten (accounteigenaar) de beschikking over een Microsoft Surface. Hierbij is Aves niet verantwoordelijk voor oneigenlijk gebruik van de accounteigenaar.

Accounteigenaar is verantwoordelijk voor veilig gebruik, dit houdt in:

- Er wordt gebruik gemaakt van Windows Hello, een sterk wachtwoord of pincode als beveiliging bij het openen of opstarten van het tablet.
- Bij verlies of diefstal meldt de accounteigenaar dit bij de directeur, welke melding zal maken bij de manager ibp, zodat accounts geblokkeerd kunnen worden.
- Zorgen dat derden niet bij “Bijzondere gegevens” kunnen. (de inloggegevens worden vaak door de computer bewaard zodat snel inloggen zonder wachtwoord mogelijk is)
- Er geen porno aanwezig is op het tablet.
- Geen illegale films, muziek of software aanwezig is op het tablet.
- Het tablet via Windows + L op slot gaat als het tablet onbeheerd achterblijft.

De directeur is verantwoordelijk voor:

- Bij vermoeden van oneigenlijk gebruik, wordt de accounteigenaar aangesproken door de directeur. De directeur heeft het recht om hierbij inzage te hebben in de gebruikshistorie.
- Verlies of diefstal wordt door de directeur aan de manager ibp gemeld.

De adviseur ict onderwijs is verantwoordelijk voor:

- Het laten ondertekenen van een gebruikersovereenkomst van de accounteigenaar.
- De gebruikersovereenkomsten archiveren in Visma.
- Verlies of diefstal van het tablet. De manager ibp maakt melding van datalek bij het CvB en het protocol datalekken zal in werking gezet worden door de manager ibp (hoofdstuk 3 Datalekken).

11. Sociale Media

Onder sociale media verstaan we:

“Sociale media is een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen”.
(Bron: https://nl.wikipedia.org/wiki/Sociale_media)

In de praktijk betekent dit dat ouders toestemming aan de school moeten geven voor het gebruik van foto's en filmpjes op de sociale mediakanalen van de school. Dit kan zijn:

- Website
- YouTube
- Twitter
- Facebook
- Etc.

De school zal dit bij de aanmelding van een leerling vragen via een toestemmingsformulier. Door te tekenen geven ouders toestemming voor het gebruik van foto's en filmpjes van hun kind op de bovengenoemde sociale media. De school is verplicht tot het jaarlijks ***benoemen*** van de overeenkomst mocht de ouder dit willen wijzigen. Dit kan bijvoorbeeld via de nieuwsbrief of de schoolgids.

Op het moment dat een ouder geen toestemming geeft, zal de school ervoor zorgdragen dat de betreffende leerling of leerlingen niet herkenbaar in beeld zullen zijn.

11.1 Gebruik software van "Bitedance Ltd"

Aves gebruikt geen TikTok of andere software van ontwikkelaar "BiteDance Ltd".
De privacy van leerlingen en medewerkers is niet te waarborgen. Het bedrijf staat bekend om het verzamelen van grote datasets van gebruikers en deze te gebruiken, zodat gebruikers beïnvloed kunnen worden. Ook is het bedrijf geclassificeerd als "spionage gevoelig" door de AIVD.
Comlog Automatisering blokkeert hierom actief het gebruik en installatie van TikTok of andere software van BiteDance Ltd op alle Aves apparaten (pc, laptops en IPads)

12. Externen

Aves verleent geen toegang tot zijn administratiesysteem (ParnasSys) aan "derden", als deze niet voor onbepaalde tijd aan Aves verbonden zijn.

12.1 GGD

De wet staat uitwisseling toe.

12.2 Kentalis

Kentalis communiceert volgens, in overeenstemming met de AVG. Emailberichten vanuit Kentalis worden versleuteld verstuurd via Cryptshare. Bij het versturen van dossiers wordt het dossier tijdelijk in een beveiligde omgeving geplaatst. Het wachtwoord wordt afzonderlijk via sms verstuurd.

12.3 Samenwerkingsverband

Er zijn afspraken met het samenwerkingsverband. Uitwisselen van leerling gegevens gebeurt via een afgesproken protocol.

12.4 IJsselgroep

De IJsselgroep communiceert in overeenstemming met de AVG.

12.5 Bibliotheek

De bibliotheek zorgt zelf voor duidelijke afspraken volgens de AVG

12.6 Foto's en video door derden

Als school heb je regelmatig te maken met ouders in de school. Veel van de ouders maken tegenwoordig gebruik van een smartphone om actuele activiteiten van hun eigen kinderen (en daarmee vaak ook dat van anderen) te verslaan. Ze maken foto's en of video's, welke met regelmaat op de sociale media terecht komen.
Als ouders foto's maken van de leerlingen tijdens een evenement op school of tijdens schooltijd, dan mogen deze ouders de foto's niet verwerken (bijvoorbeeld plaatsen op een facebookpagina) zonder dat de ouders van de leerlingen die op de foto staan hiervoor hun toestemming hebben gegeven.

Scholen van Aves informeren ouders over het maken van foto's en filmpjes tijdens schooltijd.

Op te nemen in de schoolgids:
Het is ouders/verzorgers niet toegestaan om foto's en filmpjes van kinderen, anders dan hun eigen op sociale media te verspreiden, dit geldt ook voor leerkrachten en medewerkers van de school. De school zal tijdens evenementen zelf foto's en video's maken en deze verspreiden via de eigen sociale media (website, facebook, twitter), waarbij er rekening gehouden wordt met de privacy rechten van het kind.

Bij inschrijving wordt toestemming gevraagd voor publicatie van beeldmateriaal per gebruikt medium. Hieronder vallen:
Website
Schoolgids
Sociale media
Beeldmateriaal in de school
Ouder app

Van de school wordt verlangd dat zij iedere jaar actief aandacht vraagt voor de gegeven toestemming.

13. Netwerkbeheer

Comlog Automatisering verzorgt het netwerkbeheer van alle Aves locaties. Dit beheer wordt voornamelijk op afstand gedaan. Werkzaamheden aan het netwerk op locatie worden altijd in opdracht van de adviseur onderwijs & ict gedaan en in overleg met de directeur.

14. Draadloos netwerk

Het draadloos netwerk van Aves is opgebouwd uit de volgende signalen met elk hun eigen gebruikers.

SSID	Gebruiker	Bijzonderheden
AVES-GAST	ouders, logopedist, GGD	Open tussen 7.00 en 22.00 uur
AVES-LEERKRACHT	leerkrachten	altijd open
AVES-SCHOOLNAAM	laptops	directe netwerkverbinding
AVES-LEERLING	leerlingen (BYOD)	Open tussen 8.00 en 16.00 uur

De wachtwoorden van bovenstaande signalen zijn voor AVES-SCHOOL en AVES-LEERLING uniek per locatie. De andere signalen zijn identiek voor alle locaties.

Er is bewust gekozen voor deze indeling, omdat op deze manier de wachtwoordwijzigingen simpel zijn door te voeren bij vermoeden van misbruik. Bij vermoeden van misbruik heeft Aves het recht om een rapportage op te vragen van de locatie waar er een vermoeden is van misbruik.

Aandachtspunten:

- Zorg dat een code voor gasten niet van buitenaf zichtbaar is.
- Te maken met grote groepen? Vraag een tijdelijk AVES-GAST wachtwoord aan (via Comlog). Op deze manier kan tijdens een ouderavond iedereen gebruik maken van wifi en heeft dit later geen nadelige gevolgen voor de bandbreedte. (internetgebruik gaat omhoog als ouders de school binnen komen en automatisch verbonden worden met het gast-netwerk.)

Bijlage 1 Bewaartermijnen

Gegevens in het leerling dossier

Maximaal 2 jaar nadat een leerling is uitgeschreven en 3 jaar als een leerling is doorverwezen naar het Speciaal Onderwijs.

Gegevens over verzuim en afwezigheid

Maximaal 5 jaar nadat een leerling is uitgeschreven.
Gegevens in- en uitschrijving
Noodzakelijk voor berekening van bekostiging. Maximaal 5 jaar nadat een leerling is uitgeschreven.

Gegevens bekostiging school

Minimaal 7 jaar na afloop van het schooljaar waarop de bekostiging betrekking heeft.
Gegevens met betrekking tot bezwaar-, klachten- of gerechtelijke procedure
Maximaal 5 jaar nadat leerling is uitgeschreven.

Camerabeelden

Ten behoeve van toezicht. Maximaal 4 weken, tenzij er een incident is vastgelegd.
Gegevens in personeelsdossier met betrekking tot fiscale bewaarplicht
Maximaal 5 jaar na uitdiensttreding.

Overige gegevens in het personeelsdossier

Maximaal 2 jaar na uitdiensttreding.

Gegevens over het gebruik van ICT-middelen

Microsoft365 account. Email, bestanden en andere gegevens van personeel en leerlingen
Maximaal 6 maanden.

Gegevens bij sollicitatie
Sollicitatiebrief, formulier, correspondentie over de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek.
Maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant, maximaal 2 jaar na uitdiensttreding voor benoemde collega.

Foto's en video's
Maximaal 3 jaar na opname of na intrekken toestemming.

Bewaartermijnen:
https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/bewaren-van-persoonsgegevens#:~:text=Maar%20organisaties%20mogen%20die%20gegevens,hoe%20lang%20zij%20persoonsgegevens%20bewaren

Specifiek voor leerlingdossiers:
https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/onderwijs/leerlingdossiers
Kies "Vragen over leerlingdossiers"

Bijlage 2 Wijzigingsdocument directeur

Wijziging directeur.docx (sharepoint.com)

Link beschikbaar voor CvB, staf en directeuren

Bijlage 3 Toestemmingsformulier OSO overdracht PO naar PO

Toestemmingsformulier OSO.docx (sharepoint.com)

Link beschikbaar voor CvB, staf en directeuren

Bijlage 4 Toestemming gegevensverwerking

Toestemmingsformulier gegevensverwerking.docx (sharepoint.com)

Link beschikbaar voor CvB, staf en directeuren

Bijlage 5 Toegangsbeleid Aves

Bron	Informatie	Toegang	Beveiliging
Microsoft365	Algemeen	Medewerker Aves	Twee-staps-verificatie
SharePoint Bestuur	Documenten Organisatie, personeel, financieel, resultaten, zorg, beleid	Staf	Rechtenmatrix bepaalt niveau toegang.
SharePoint School	Documenten Organisatie, personeel, financieel, resultaten, zorg, beleid	Leerkrachten, onderwijsondersteuners, ib en directeur	Rechtenmatrix bepaalt niveau toegang
SharePoint leerling	Onderwijsresultaten, persoonsgegevens	Leerkrachten, onderwijsondersteuners, ib en directeur	Twee-staps-verificatie
ParnasSys Bovenschoolse module	Bijzondere persoonsgegevens en onderwijsresultaten	PZ, cvb (Onderwijs) en Adviseurs Onderwijs	Twee-staps-verificatie en rollen ParnasSys
ParnasSys schoolniveau	Bijzondere persoonsgegevens en onderwijsresultaten	Directeur, Ib'er, leerkracht, WPO (beperkt), trainee, onderwijsondersteuner en administratieve ondersteuning	Twee-staps-verificatie en rollen ParnasSys
Grippa	Bijzondere persoonsgegevens en onderwijsresultaten	PZ, Ib'ers scholen, TC	Twee-staps-verificatie
Visma	Persoonsgegevens	PZ, medewerkers Aves (beperkt)	Twee-staps-verificatie
Tobias	Financiën	CvB, Administratief medewerker staf, directeuren	
Spend Cloud	Financiën	CvB, Administratief medewerker staf,	

		Onderwijsadviseurs, directeuren	
Methode software	Onderwijsresultaten, persoonsgegevens	Leerkrachten, ib, directeur, onderwijsondersteuners	Twee-staps-verificatie per 1-10-2023
Website Aves	Organisatie en beleid	Adviseur onderwijs & ict, Administratief medewerker staf	
Social Media Aves (Facebook, LinkedIn, Youtube)	Organisatie en beleid	PZ, Adviseur ICT Onderwijs en Administratief medewerker staf	
Schooldossier (ISD)	Administratief medewerker staf	Directeur, Administratief medewerker staf	
Draadloos netwerk NetGear	Technische informatie verbonden devices	Adviseur onderwijs & ict en Le Fevre ICT	
Netwerk	Technische informatie verbonden devices	Comlog, Le Fevre ICT, Adviseur onderwijs & ict, Directeur en ict'er	Gesloten patchkast

Bijlage 6 Jaarplan IBP school

Wie	Wat	Waar	sept	febr	Check	Extra
dir	Overzicht rechten SharePoint	Rechtenmatrix	x	x	Manager ibp	
dir	Groepsautorisatie + accountcontrole	ParnasSys	x	x	Manager ibp	
dir	Toestemming vastleggen/wijzigen foto- en filmbeelden	Communicatie app	x		Manager ibp	Een keer per jaar ouders er aan herinneren via nieuwsbrief en standaard opnemen in schoolgids
dir	Actief informatie aan ouders hoe omgaan met privacy		x		Manager ibp	
dir	Vernietigen leerling dossiers	ParnasSys	x		Manager ibp	Handleiding ParnasSys
Ik	Vernietigen foto's	Website, SharePoint, OneDrive	x		dir	Extra aandacht voor foto's op mobiele telefoons.
ict	Leerlinggegevens bij verwerkers verwijderen.	Softwareleverancier die niet gekoppeld is aan Basispoort	x		dir	
dir	IBP beleid is jaarlijks themabespreking in team			x	dir	Aandacht voor datalekken en hoe te handelen. Verwijderen foto's. Toegang tot documenten. Nieuwe software melden. Geheimhouding Opschonen mailbox

				Protocol gescheiden ouders
dir/lk	Verwijderen sollicitatiebrieven etc., getuigschrift, verklaring omtrent gedrag	OneNote	indien van toepassing	Informatie sollicitant wordt via OneNote gedeeld.
ib	Toestemming vastleggen uitwisseling persoonsgegevens met derden (zoals orthopedagogen/psychologen)	ParnasSys	Indien van toepassing	Brief met handtekening in leerling dossier uploaden

Bijlage 7 Jaarplan IBP Bestuur

Wie	Wat	Wanneer	Check	Extra info
Manager ibp	Evaluatie ibp beleid	Juni	Cvb	
PZ	Vernietigen personeelsdossiers	September	Manager HRM	2 jaar na eind dienstverband. Tenzij werkgever belanghebbende is bv. in het kader van een rechtszaak
Secretariaat	Sollicitatiebrieven, -formulieren, correspondentie omtrent de sollicitatie, getuigschriften en verklaring omtrent gedrag	incidenteel	Manager ibp	4 weken zonder toestemming, 1 jaar met toestemming van de sollicitant na beëindiging procedure. Tenzij sollicitant werknemer wordt dan mogen de gegevens tot een jaar na uitdiensttreding worden bewaard
PZ	Check Toegang ParnasSys (medewerkers uit dienst)	September	Directeur	
Manager ibp	Gegevens over datalek	September	FG	Gemeld aan betrokkenen minimaal 1 jaar advies 3 jaar
Manager ibp	Rechtenmatrix bestuur	September	FG	
Manager ibp	Overzicht incidenten naar bestuurder	Juni	Cvb	
Financiën	Financiële administratie verwijderen	Na accountantscontrole	Cvb	7 jaar vanaf datum opstellen
Financiën	Leerlingen tellingen	Na accountants controle	Cvb	Bewaartermijn 7 jaar
Manager ibp	Softwarelijsten controleren	Juni	FG	

Manager ibp	Verwerkingsregister bijwerken	Na controle softwarelijsten	FG
Manager ibp	Verwerkingsovereenkomsten	Na controle softwarelijsten	FG
Manager ibp	AVG onder aandacht alle medewerkers houden	Oktober	FG
Manager ibp	Bewaartermijnen overzicht bijwerken	Oktober	FG