Werkveld	Datum	Instemming/Advies GMR	Vastgesteld CvB
ICT	11 december 2019	A - 11 december 2019	13 januari 2020

2.8.2 | Handboek IBP

Privacy gedragsregels en afspraken

Inhoudsopgave

1. Toegang ParnasSys

Alleen leerkrachten en administratief medewerkers van Aves krijgen, door Personeelszaken, toegang tot ParnasSys voor de locatie waar zij op dat moment werkzaam zijn. Zij maken gebruik van de twee-staps verificatie en krijgen toegang tot alle groepen. (Kan een leerkracht geen gebruik maken van de twee- staps verificatie, dan wordt de toegang door de directeur beperkt tot de leerkracht eigen groep)

Er is een uitzondering voor WPO studenten. WPO studenten zullen tijdens de stageperiode toegang krijgen 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 geschiedt.

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

1.1 Doelbepaling en doelbinding

Gezamenlijke verantwoordelijkheid voor de ontwikkeling van onze leerlingen (denk daarbij ook aan Unit-onderwijs of TOM-onderwijs e.d.) betekent dat iedere leerkracht ook de mogelijkheid moet hebben om van leerlingen die niet tot zijn of haar groep behoren verslaglegging te kunnen doen van bijvoorbeeld incidenten of oudergesprekken. Resultaten moet bekeken en geanalyseerd worden om tot goede ondersteuningsplannen te kunnen komen. Het huidige aanbod van invalleerkrachten is niet toereikend, het gevolg is dat regelmatig klassen moeten worden opgedeeld. Het is voor de leerkracht dan noodzakelijk bij de gegevens van de leerlingen te kunnen.

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.

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.

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 accountbeheer.

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 (adviseur ICT Onderwijs).

1.6 Accountbeheer

Alle ParnasSys accounts zijn georganiseerd via de bovenschoolse module. De medewerker krijgen van PZ een bestuur aanstelling 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 privacy gevoelige informatie. Dit betekent dat een ParnasSys account middels een sterk wachtwoord door de gebruiker is beveiligd, maar dat vanaf 01-01-2020 er ook gebruik gemaakt gaat worden van een twee-staps-verificatie voor alle accounts. Dit betekent dat de gebruiker een extra verificatie code krijgt op zijn of haar smartphone.

https://ParnasSys.zendesk.com/hc/nl/articles/210119605

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 de telefoon goed beveiligd is met een pincode, sterk wachtwoord, vingerafdruk of irisscan. Bij verlies of

diefstal van de mobiele telefoon, welke voorzien is van deze informatie dient aangifte gedaan te worden en moet er binnen 24 uur melding gemaakt worden bij de adviseur ict onderwijs 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.

Bewaartermijnen:
https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/onderwijs/leerlingdossiers

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

WPO studenten en zij-instromers krijgen een Microsoft365 account, aangezien zij contractueel aan de school verbonden zijn en zij als volwaardig leerkracht moeten kunnen functioneren. PZ is verantwoordelijk voor het aanvragen van een medewerker account (met rechten op het schoolportaal) via help@comlog.nl. Aangezien dit niet geautomatiseerd kan worden, is het van belang dat de directeur dit Microsoft365 account ook weer laat verwijderen, bij het beëindigen van het WPO contract. (via help@comlog.nl)

Ook zullen zij een ParnasSys account ontvangen en gekoppeld worden aan de school. Zij zullen echter alleen toegang krijgen tot de eigen groep en zullen gebruik moeten maken van de twee-staps verificatie. Hiervoor is de directeur verantwoordelijk.

Voor studenten geldt een geheimhoudingsverklaring als het gaat om privacy gevoelige 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 en 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 software leveranciers.
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

Bovenstaande verbeterpunten zullen door de stuurgroep opgepakt worden.

4. Datalekken

Alle mogelijke vormen van datalekken dienen binnen 72 uur gemeld te worden bij de Manager IBP van Aves (R. Heupink) , welke melding zal maken bij het meldloket datalekken bij de Autoriteit Persoonsgegevens. Informatie is ook te vinden op de website van Aves. Er is tevens een speciaal emailadres (privacy@aves.nl) aangemaakt voor het melden of voor eventuele vragen rondom privacy. In dit hoofdstuk staat beschreven hoe Aves omgaat met mogelijke datalekken.

Gebruikte termen:

- Beveiligingsincident; een beveiligingsincident is een gebeurtenis die er voor 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 ; r.heupink@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 omtrent 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):

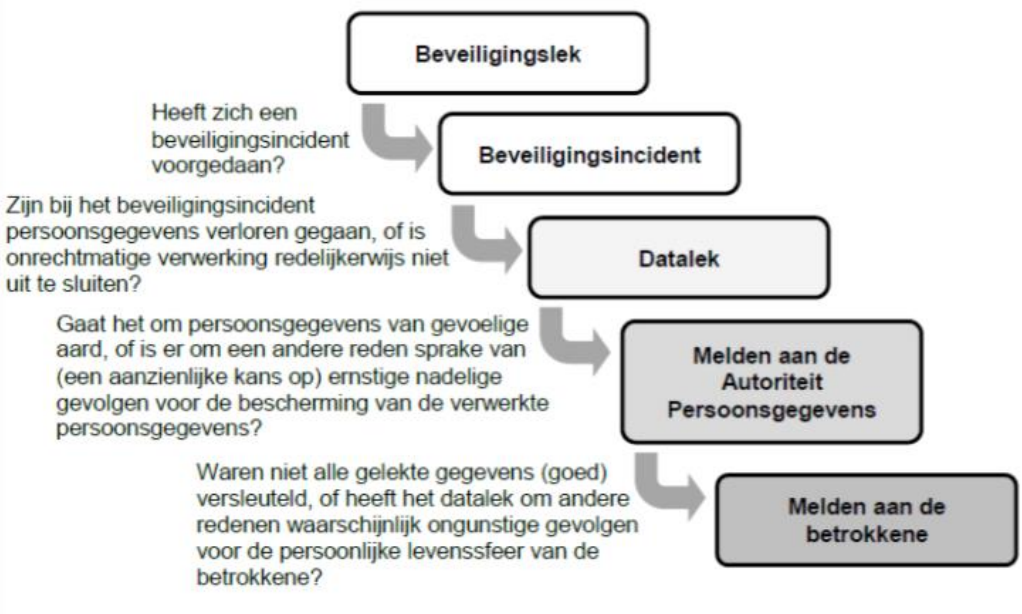
- Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
- Datum/periode van het beveiligingsincident
- Aard van het beveiligingsincident
- Wanneer van toepassing (bij een datalek):
- Omschrijving van de groep 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

Indien 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 er vanuit 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 (server, schoolportaal, OneDrive voor bedrijven, ParnasSys). Memory sticks worden niet gebruikt.
- Toestemming voor gebruik software aanvragen. Om te voorkomen dat er software programma'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 6. Als een school een nieuw programma wil gebruiken die niet in de lijst voor komt, moet contact opgenomen worden met de adviseur ict onderwijs.
- Veilig mailverkeer. Het versturen van documenten met persoonsgegevens via e-mail is niet toegestaan. Beveiligde documenten mogen als bijlage, afzonderlijk van het wachtwoord, verzonden 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 adviseur ict onderwijs 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 informatie gegevens 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
Unilogic
ParnasSys (hieronder valt ook Zien)
Rolfgroep
Gynzy
Blink
Noordhoff
Digikeuzebord
Zwijsen
Thieme Meulenhoff
Malmberg
WIS
Aerohive
Microsoft
Snappet
Onderwijs Bureau Meppel
Cito
Bloon
ZuluConnect
Momento
Prowise
Kennisnet Entree
IEP
Route 8
Overstap Service Onderwijs (OSO)
Onlineklas
Rovict (SCOL)
Rolfgroep CMS
Schoolsupport
DHH
Entree, nummervoorziening
Onderwijsadvisering ivm drempelonderzoek
AMN systems

Dedicom
Foto Koch
Kindkans
Klasseplan
Konnect
Logo3000
SchouderCom
Schoolwise (Flevomeerbibliotheek)
Mijn Rapportfolio
ZuluDesk
IJsselgroep
Vensters PO
Peppels (Tienercollege)
Schoolfoto
Kanvas LVS (Kanjertraining)
Nieuwe schoolfoto
Dorr Onderwijs BV

Deze lijst zal door de Manager IBP continu bijgewerkt worden.

6. Toegangsbeleid gegevens en applicaties

6.1 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 dienen een goed wachtwoord te kiezen 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.)
Een standaard Aves wachtwoord wordt niet geaccepteerd als persoonlijk wachtwoord van een medewerker.

6.2 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 streven er naar om een sterk wachtwoord te gebruiken 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.

6.3 Twee staps verificatie Microsoft 365

Aves onderkent het belang van goede beveilig op systemen met privacy gevoelige informatie. Om deze reden zal de Microsoft365 omgeving van de medewerker vanaf 1-8-2020 allemaal voorzien zijn van een twee factor authenticatie. Aves zal dit gefaseerd invoeren om de medewerkers hieraan te laten wennen (en onderzoekt de verschillende varianten van twee staps verificatie evenals de impact van beveiliging en gebruiksgemak). Samen met Microsoft en Comlog onderzoeken we de mogelijk om “Windows Hello for bussines” in te zetten op het persoonlijk device van de leerkracht, zodat gebruiksgemak en veiligheid beide gewaarborgd zijn.

6.4 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 adviseur ict onderwijs via privacy@aves.nl , welke een mededeling zal verspreiden om herhaling te voorkomen.

7. Expertise centrum

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 Expertise centrum, 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 aanmeldformulier worden opgenomen. Het is tevens opgenomen in het document “Toestemming gegevensverwerking”

9. Overstapservice Onderwijs (OSO)

Aves maakt gebruik van ParnasSys als leerling administratie systeem. In ParnasSys zit privacy gevoelige 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, welke door de gebruiker ondertekend zal worden.

Aves onderzoekt de mogelijkheid om het tablet via Microsoft Intune te gaan beheren. Niet eerder dan 1-1-2020 zal dit operationeel zijn. Beheer via Intune zal zorgdragen voor veiligheid van

documenten middels een Bitlocker encryptie van de harde schijf. Alle tablets zullen op deze manier vanaf 1-3-2020 ingericht en beheerd worden door Comlog.
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 en verwijzen we naar het Protocol social media/internet/email, paragraaf 2.9 (zie bijlage 2).

Accounteigenaar is verantwoordelijk voor veilig gebruik, dit houdt in:
- Er wordt gebruik gemaakt van 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 achter blijft.

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 bovenschools ICT' er gemeld.

De adviseur ict onderwijs is verantwoordelijk voor:
- Het laten ondertekenen van een gebruikersovereenkomst van de accounteigenaar.
- De gebruikersovereenkomsten archiveren op het Aves kantoor.
- Verlies of diefstal van het tablet. De adviseur ict onderwijs 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 media kanalen 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, een voorbeeld is te vinden in de bijlage. Door te tekenen geven ouders toestemming voor het gebruik van foto's en filmpjes van hun kind op de bovengenoemde sociale media. Tevens verplicht de school zich hiermee 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 zorg dragen dat de betreffende leerling of leerlingen niet herkenbaar in beeld zullen zijn.

12. Externen

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

12.1 GGD

De wet staat uitwisseling toe.

12.2 Kentalis

Kentalis communiceert conform 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 conform de AVG.

12.5 Bibliotheek

De bibliotheek zorgt zelf voor duidelijke afspraken conform 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 verlangt dat zij iedere jaar actief aandacht vraagt voor de gegeven toestemming.

13. Netwerkbeheer

De Rolfgroep verzorgt het netwerkbeheer van alle Aves locaties. Dit beheer wordt voornamelijk op afstand gedaan. Voor directie, beheer, leerkrachten, ib, leerlingen en gasten is er een omgeving, welke beschermd is via een wachtwoord. De Rolfgroep hanteert hiervoor “standaard” wachtwoorden. Het wachtwoord voor de beheeromgeving is door Aves aangepast en bij de ict’ers en de adviseur ict onderwijs bekend. Bij vermoeden van misbruik is de adviseur ict onderwijs gerechtigd dit wachtwoord door de Rolfgroep aan te laten passen voor alle scholen.

De omgeving voor de directie is wat beter beschermd dat de andere omgeving. De documenten van de directie zijn door niemand, behalve de Rolfgroep, benaderbaar. Bij een wisseling van directie is het noodzakelijk om dit schriftelijk door te geven middels het wijzigingsdocument directeur.

Op iedere locatie is er een leraar met ICT taken die geschoold is in het gebruik van het netwerk en in het bezit is van de beheer inloggegevens. Er wordt alleen van de beheeromgeving gebruik gemaakt als dit noodzakelijk is.

Leerkrachten werken in een algemene of persoonlijke omgeving. De school is vrij in het aanpassen van het leerkracht wachtwoord. Dit kan door de ICT’er gedaan worden (eventueel met ondersteuning van de Rolfgroep).

Het advies is om iedere gebruiker (leerkracht) een eigen account te geven met een wachtwoord dat bekend is via de (school) ict’er. Op deze manier kan ook de OneDrive koppeling gemaakt worden in Office2016 zonder dat deze gegevens voor anderen beschikbaar zijn.
De Ib’er van de school heeft een eigen omgeving waarin gewerkt wordt. Mocht de Ib’er op meerdere locaties werken en gebruik maken van een eigen (door de Rolfgroep ingerichte) laptop, dan is het mogelijk deze zo in te richten dat er met 1 gebruikersnaam en wachtwoord toegang wordt verleend aan de ib omgeving van de Rolfgroep.

Leerlingen hebben een eigen afgesloten omgeving op het netwerk. Zij loggen in met standaard gebruikersnamen en wachtwoorden passend bij de groepen. Het is voor leerlingen niet toegestaan om (zonder toezicht van de leerkracht) van een andere omgeving dan “leerling” gebruik te maken.

Gasten kunnen ook een plek krijgen binnen het netwerk. Deze omgeving is volledig afgeschermd. Het is niet mogelijk om via deze omgeving bij de documenten op de server te komen.

13.1 Afstandsbediening

De Rolfgroep heeft een systeem voor inloggen op de server terwijl je niet op school bent. Hiervoor is het nodig om het programma “Afstandsbediening” te downloaden.
http://www.derolfgroep.nl/content/overige-downloads/overige-downloads.aspx
Na installatie moeten de gegevens van de server ingevoerd worden, zodat het programma contact kan maken met de server. De gegevens voor deze “Afstandsbediening” zitten standaard in de map “Afstandsbediening” op de K: schijf van de directeur. Hierdoor zijn deze gegevens niet vrij toegankelijk. Na invoering van de gegevens kan de gebruiker een computer van de school “overnemen” en inloggen met de voor hem of haar bekende inloggegevens.

Als een leerkracht gebruik wil maken van deze afstandsbediening, dan kan hij of zij dat bij de ict’er en de directeur aangeven. De ict’er kan via de beheer omgeving een certificaat op naam uitgeven, zodat de betreffende leerkracht gebruik kan maken van de “Afstandsbediening”. De ict’er en de directeur zijn verantwoordelijk voor het intrekken van het certificaat op het moment dat de betreffende leerkracht geen toegang meer mag hebben tot de schoolserver.

Bij vermoeden van misbruik van de beheeromgeving dient melding gemaakt te worden bij de adviseur ict onderwijs.

Na de implementatie voor het bestuurs- en schoolportaal zullen alle documenten in de “Cloud” staan van Mijn Onderwijs Portaal. Dan vervalt deze paragraaf.

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
ROLF – Brinnr	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 vanuit de hivemanager van Aerohive een rapportage op te vragen van de locatie waar er een vermoeden is van misbruik.

Omdat het signaal AVES-SCHOOLNAAM verbonden is met de server is het niet toegestaan om het wachtwoord aan externen te overhandigen.

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 de Rolfgroep). 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.)

- *Gelijktrekken van de signalen voor de oud SCPO scholen, aanpassen benaming Gast signaal is hierbij noodzakelijk . Migratie hyvemanager zal plaatsvinden als dat noodzakelijk is om extra werk te voorkomen.*

15. Rechtenmatrix Algemeen

Onderwerp	Beheer	Toegang
Microsoft365	Comlog	Directeur, staf
Bestuursportaal	Comlog	Rechtenmatrix via Adviseur ICT Onderwijs beschikbaar
Schoolportaal	Comlog	Rechtenmatrix via directeur en school ict'er beschikbaar
ParnasSys Bovenschoolse module	PZ	PZ, CvB (Onderwijs) Adviseurs Onderwijs
ParnasSys schoolniveau	PZ en Directeur	Directeur, Ib'er, leerkracht, WPO (beperkt), administratieve ondersteuning
Netwerk	Rolfgroep	Directeur, leerkracht, WPO, administratieve ondersteuning
Grippa	PZ	PZ, Ib'ers scholen, TC
ZuluConnect	Rolfgroep	Directeur, leerkracht, WPO
Website Aves	Rolfgroep	Adviseur ICT Onderwijs, Administratief medewerker staf
Social Media Aves (Facebook, LinkedIn, Youtube)	PZ, Adviseur ICT Onderwijs en Administratief medewerker staf	PZ, Adviseur ICT Onderwijs en Administratief medewerker staf
Raet	OBM	PZ, medewerkers Aves (beperkt)
Tobias	OBM	CvB, Administratief medewerker staf, directeuren
Pro Active	OBM	CvB, Administratief medewerker staf,

		Onderwijsadviseurs, directeuren
Schooldossier (ISD)	Administratief medewerker staf	Directeur, Administratief medewerker staf
Aerohive (wifi)	Rolfgroep	Adviseur ICT Onderwijs

16. Bijlage 1; Wijzigingsdocument directeur

https://skofvportaal.sharepoint.com/:w:/s/mop-40662-aves/Documenten/6Organisatie/EcfnXSJHsO5JsuDlMeSPFTABZZPmhgN3FnXyxfrFZOE48w?e=4UE1Uz

Link beschikbaar voor CvB, staf en directeuren

17. Bijlage 2; Toestemmingsformulier OSO overdracht PO naar PO

https://skofvportaal.sharepoint.com/:w:/s/mop-40662-aves/Documenten/6Organisatie/ET-7pHzKiIlOqdoe6NIzddgBMfL0_N6jU75NBjKWcO42Xw?e=3R8J1q

Link beschikbaar voor CvB, staf en directeuren

18. Bijlage 3; Toestemming gegevensverwerking

https://skofvportaal.sharepoint.com/:w:/s/mop-40662-aves/Documenten/6Organisatie/EelJF8UsL7RBtQtR2BORDm8BxIaZN-MAKqCqC8PKj1f_7Q?e=FyyJHJ

Link beschikbaar voor CvB, staf en directeuren