Veiligheidsbeleidsplan csg Jan Arentsz 2024-2025

Inleiding

Csg Jan Arentsz wil in de regio herkend worden als een school met een warm en duidelijk schoolklimaat.
Een school met een grote mate van organisatietrots, met medewerkers en leerlingen die zich gewaardeerd voelen. Die zich veilig voelen. Met onderwijs dat een wezenlijke bijdrage levert aan de kwaliteit van het leven van individuen en van de samenleving, dat zich richt op kwalificatie, socialisatie EN persoonsvorming! Met een schoolleiding die zorgt voor duidelijke richtlijnen, die inspireren en ondersteunen daar waar nodig is. Een school ook met een platte organisatie waarin de middelen efficiënt worden aangewend, waardoor bureaucratische omwegen worden voorkomen.

Binnen de CSG Jan Arentsz zijn afspraken gemaakt over de wijze waarop uitvoering wordt gegeven aan deze collectieve ambitie. Essentieel is daarbij dat wordt gewerkt volgens het principe: 'trust me, prove me'. Vertrouwen is de basis van alle relaties binnen de school en moet zorgen voor een cultuur van 'veilige onzekerheid'. Vestigingen, teams, secties, hebben de ruimte om keuzes te maken in de uitvoering. Daarbij is fouten maken onvermijdelijk. Het vertrouwen in de verantwoordelijkheid en deskundigheid van alle betrokkenen om te leren van die fouten is groot. Tegelijkertijd is de ruimte die er is niet onbegrensd. We hebben een aantal gemeenschappelijke afspraken. En in het licht van dit document zijn de afspraken die betrekking hebben op hoe we met elkaar omgaan leidend.

- We praten met elkaar en niet over elkaar
- We houden verstoringen zo klein mogelijk
- We ruimen oud zeer zo snel mogelijk op
- We blijven met elkaar in gesprek ook als het moeilijk wordt
- We stellen onze mening uit totdat we volledig zijn geïnformeerd
- We nodigen iedereen die iets heeft bij te dragen uit om mee te praten
- We geven het goede voorbeeld
- We accepteren geen discriminatie in welke vorm dan ook
- We gaan vertrouwelijk om met vertrouwelijke informatie
- We mogen elkaar aanspreken op afspraken en doen dat op een veilige manier

'Trust me, prove me' betekent niet dat er blind vertrouwen is. 'Prove me' houdt in dat alle betrokkenen bereid zijn verantwoording af te leggen over de keuzes die gemaakt zijn.

Het veiligheidsbeleidsplan kan gezien worden als een kerndocument. Uitwerkingen van de principes die hier beschreven zijn, vinden plaats in hiervan afgeleide documenten.

1. Gedragscode
2. Richtlijnen voor buitenschoolse activiteiten
3. Pestprotocol
4. Camerabewaking
5. Het doen van aangifte
6. (Seksuele) intimidatie en (seksueel geweld)
7. Spijbelen en verzuim
8. Ongewenst bezoek schoolterrein
9. Zorgvuldig omgaan met sociale media
10. Datalek
11. informatiebeveiliging en privacy beleid
12. Privacyreglement
13. Wat als je een zwakke plek vindt in onze systemen

Alle documenten zijn te lezen op de website onder de button veiligheid.

Algemene opmerkingen

1. Dit Veiligheidsbeleidsplan geldt voor alle vestigingen van de CSG Jan Arentsz. De afspraken en voorschriften gelden in de gebouwen, op het schoolterrein rond de gebouwen en tijdens alle door de school georganiseerde activiteiten elders.
2. Op het schoolterrein zijn camera's opgehangen ter preventie van crimineel en grensoverschrijdend gedrag.
3. De kluisjes binnen school mogen op elk moment geopend worden door daartoe door het bevoegd gezag gemachtigde personen, als er een vermoeden bestaat dat de inhoud daarvan in strijd is met schoolafspraken dan wel met wet- en/of regelgeving. Ook tassen, jassen en andere persoonlijke eigendommen mogen geopend en gecontroleerd worden.
4. Alle incidenten waarbij de rust en de veiligheid van de schoolgemeenschap in het geding is worden gemeld in het incidentenregistratiesysteem van Magister. We maken een onderscheid tussen "incidenten" en "wettelijke incidenten" .Een schoolleider of een collega namens deze zal deze registratie verzorgen. Dat laat onverlet dat melding van incidenten door een ieder kan plaatsvinden die hiermee in aanraking komt. Incidenten kunnen ook worden gemaild aan: veiligheid@ja.nl

   Te denken valt hierbij aan (niet uitputtend):
   - Spijbelen
   - (Digitale)Fraude
   - Vandalisme
   - Pesten
   - Discriminatie
   - Bedreigingen
   - Vechtpartijen
   - Mishandeling
   - Wapenbezit waaronder messen
   - Seksuele intimidatie, seksueel geweld
   - Diefstal, heling
   - Gebruik van verslavende middelen of de handel daarin
   - Vuurwerkgebruik in alle categorieën
   - Informatiebeveiliging en privacy

Het gaat hier om incidenten en gedragingen die de rust en de veiligheid verstoren, waarmee de wet wordt overtreden of die niet passen in een cultuur van vertrouwen. We vragen van alle personeelsleden, leerlingen en hun ouders/verzorgers om in deze cultuurdrager te zijn. Het is goed dat we ons steeds afvragen of het grensoverschrijdende gedrag een signaal is voor een dieperliggend probleem. Is dat het geval dat komen zorgteam en externe partijen in beeld die hierbij kunnen helpen. De schoolleider doet melding in het incidentenregistratiesysteem van alle hierboven genoemde zaken, of draagt er zorg voor dat dit wordt gedaan.

De school is niet verantwoordelijk voor elke vorm van materiële en immateriële schade veroorzaakt door welke vorm van grensoverschrijdend gedrag dan ook. Is er sprake van schade door toedoen van een leerling, dan is de leerling (dan wel zijn ouder(s)/verzorger(s)) aansprakelijk voor de schade. Bij ernstige vormen van grensoverschrijdend gedrag wordt aangifte gedaan, dan wel wordt leerling en/of de ouders/verzorgers geadviseerd aangifte te doen.

Uiteraard heeft het Jan Arentsz een ontruimingsplan en een BHV team. De ontruimingsplannen zijn bekend bij onze medewerkers. Leerlingen vinden de informatie die zij nodig hebben op de deuren van de klaslokalen en op de ontruimingsplattegronden. Ontruimingen worden regelmatig geoefend.

Bijlagen

1. Gedragscode

Deze code zal jaarlijks worden geëvalueerd in overleg met de PMR:

- We gaan respectvol met elkaar om in woord, gebaar en houding;
- We zorgen met elkaar voor een veilig klimaat waarin voor alle medewerkers en leerlingen ruimte is om hun gevoelens, overtuigingen en meningen op een respectvolle manier kenbaar te maken;
- We geven het goede voorbeeld;
- We spreken met elkaar en niet over elkaar;
- Professioneel gedrag blijkt ook uit onze kledingkeuze;
- We accepteren geen discriminatie in welke vorm dan ook;
- We bewaren en bewaken een professionele afstand tussen personeel en leerling;
- We zijn samen verantwoordelijk voor een schoon, veilig en sociaal schoolklimaat;
- We gaan vertrouwelijk om met vertrouwelijke informatie;
- We mogen elkaar aanspreken op de afgesproken regels en we doen dat op een veilige manier.

2. Buitenschoolse activiteiten

Algemeen
Er is een digitaal formulier opgesteld om buitenschoolse activiteiten zo veilig mogelijk te doen verlopen. Dit formulier dient voorgaande aan een activiteit doorgenomen en ingevuld te worden. Het is terug te vinden op het medewerkersportaal, onder het kopje “Buitenschoolse activiteiten”.

Controlelijst voor buitenschoolse activiteiten

1. **<u>Voorbereiding</u>**

- De bestemming wordt gecheckt op de site van de Rijksoverheid m.b.t. het reisadvies.
- De schoolleider heeft toestemming gegeven ten aanzien van programma, doelgroep, begeleiding, doelstelling, bestemming, begroting en consequenties met betrekking tot de organisatie;
- De schoolleider wordt op de hoogte gehouden van alle relevante reisdetails (zoals begeleiding, vervoer, verblijfplaats, contactmogelijkheden);
- De meldkamer is op de hoogte gebracht van de leerlingen die meegaan, de receptie is op de hoogte gebracht van de activiteit.
- Voor de activiteit wordt een begroting gemaakt (kosten vervoer, kosten entree, kosten consumpties, overige kosten, aantal deelnemende leerlingen, eventueel bijdragen van de school, bedrag per leerling)

2. **<u>Begeleiding</u>**

- Er is voldoende begeleiding om toezicht te houden.

3. **<u>Calamiteiten</u>**

- Er gaat een volledige EHBO-doos mee op excursie (bij kamp, werkweek of sport/buitenactiviteit).
- Het is bekend welke leerlingen medicijnen gebruiken.
- In geval van wangedrag en wanneer ernstige disciplinaire maatregelen worden overwogen, wordt de schoolleider onmiddellijk geraadpleegd. In overleg wordt bepaald wat er dient te gebeuren.

4. **<u>Ouders/verzorgers en leerlingen</u>**

- Met de leerlingen is besproken hoe te handelen bij calamiteiten en/of incidenten.
- Alle essentiële informatie ten aanzien van programma, bereikbaarheid, regels en afspraken is aan de ouders/verzorgers en leerlingen doorgegeven.
- Alle ouders/verzorgers hebben in het geval van een meerdaagse activiteit schriftelijk toestemming gegeven.

3. Pestprotocol

Op het Jan Arentsz vinden we het belangrijk dat zowel leerlingen als personeel in ieder geval onze drie waarden naleven:

1. Wij hebben respect voor elkaar
2. Wij helpen elkaar
3. Wij nemen onze verantwoordelijkheid

Op het Jan Arentsz mag je allemaal anders zijn. Vanaf het moment dat een leerling binnenkomt krijgt hij alle ruimte om zich te ontplooien, maar nooit ten koste van anderen. Iedereen heeft een stem en we willen ook dat iedereen leert luisteren. We verwachten van Jan Arentsz leerlingen dat ze zelfstandig zijn of worden en we helpen de leerlingen ook als ze daar begeleiding bij nodig hebben om dat te leren. Je bent meer dan de cijfers die je haalt bij ons op school.

Preventieve aanpak

Pesten past niet in deze visie en hier geldt: voorkomen is beter dan genezen. Om die reden investeren we in de brugklas en ook in de tweede klas in preventie. De mentoren besteden regelmatig aandacht aan de wijze waarop leerlingen met elkaar omgaan. Goed investeren in preventie betekent dat je achteraf niet of weinig hoeft in te grijpen.

Een onderdeel van de preventie is 'elkaar leren kennen'. Immers, als je elkaar kent, komt pesten niet in je hoofd op. De toekomstige brugklasleerlingen maken met elkaar en de mentor kennis voor de zomervakantie. Na de zomervakantie zijn er twee introductiedagen om de groepsvorming te bevorderen.
De mentor besteedt regelmatig aandacht aan de wijze waarop de leerlingen in de klas met elkaar omgaan, waardoor er een sfeer ontstaat waarin het melden van pesten in alle veiligheid kan gebeuren.

Bij verschillende vakken of in diverse projecten wordt via de lesstof begrip gekweekt voor leerlingen die anders denken, waardoor respect ontstaat voor anderen.

Tijdens de lessen Lichamelijke Opvoeding wordt er gedurende een aantal weken nadrukkelijk aandacht besteed aan weerbaarheid en groepsvorming.
'Pestbeleid' staat niet op zich. De pedagogische aanpak heeft grote invloed op het functioneren van de groep. Al die onderdelen van het schoolwerk die bijdragen aan een groter gevoel van veiligheid dragen bij aan een warm en sociaal schoolklimaat.

Curatieve aanpak

<u>In de klas</u>

Hoe gaan we om met gesignaleerd pestgedrag? Een docent merkt dat een leerling duidelijk het slachtoffer is bij vervelende opmerkingen in de klas. Hij wordt bijvoorbeeld openlijk vernederd of verlaat huilend het lokaal en uit het gesprek blijkt dat hij als zondebok behandeld wordt. Als de docent niets doet, geeft hij daarmee aan dat hij het gedrag van de agressoren accepteert. Hij zal de leerlingen dus moeten confronteren met hun gedrag. Hij gebruikt de confronterende methode.

In een andere situatie heeft de docent alleen nog maar een (eventueel sterk) vermoeden dat het verschijnsel in een klas speelt. Dat maakt hij op uit allerlei signalen: briefjes, blikken, (zogenaamd leuke) opmerkingen in de richting van steeds dezelfde leerling. Het heeft in deze situatie weinig zin de klas met dit gedrag te confronteren: ze zullen ontkennen. De docent zal dan omzichtiger te werk moeten gaan, een directe confrontatie vermijden, maar het onderwerp indirect aan de orde stellen. Hij gebruikt dan de niet-confronterende methode.

In alle gevallen informeert de docent de mentor van de klas. De mentor kan met de leerjaarcoördinator overleggen wat een goede aanpak is. De ondersteuningscoördinator heeft vanuit zijn expertise veel kennis van zaken en kan meedenken over een aanpak in de klas.

Gesprekken buiten de klas

Omdat het pesten vooral in een groep plaatsvindt is het van cruciaal belang om het pesten ook daar aan te pakken. Daarnaast zullen er gesprekken met de gepeste leerling, de pester(s) en eventueel ouders plaatsvinden. Er zijn voor de diverse gesprekken tips beschikbaar. Daarin staan de grondhouding, het doel van het gesprek, de gespreksfasen en de voorwaarden opgesomd:

a. Gesprek met het slachtoffer

b. Gesprek met de pester

c. Gesprek tussen pester en slachtoffer

d. Aanbevelingen voor gesprekken met ouders

Er kan in dit alles een opbouw zitten. De mentor kan dat met zijn/haar leerjaarcoördinator doorspreken. Soms kan namelijk een eenmalig gesprek tussen pester en slachtoffer en het informeren van de ouders van het slachtoffer voldoende zijn. Herhaalt het pesten zich, dan is ook een gesprek met de ouders van de pester en/of slachtoffer nodig. Sancties voor de pester kunnen dan vaak ook niet uitblijven.

Indien nodig wordt er binnen of buiten de school een vorm van ondersteuning gezocht voor de pester en/of slachtoffer.

4. Protocol camerabewaking

De schoolleiding van CSG Jan Arentsz vindt bescherming van eigendommen van de school en de schoolgebruiker belangrijk. Naast persoonlijke surveillance wordt gebruik gemaakt van camerabewaking in en rond de school.

Het doel van de camerabewaking is:

- Het beschermen van de schooleigendommen en de eigendommen van de gebruikers van de school;
- Preventie tegen vandalisme;
- Het bevorderen van het veiligheidsgevoel van de gebruikers van de school.

Gebruik van de camera:

- De camera's worden alleen gebruikt om te waken over de eigendommen en de veiligheid van de school en de schoolgebruiker;
- Bij de ingangen van het schoolterrein staan waarschuwingsborden met betrekking de camerabeveiliging.

Bewaren van de opgenomen informatie:

- De opgenomen informatie wordt één week bewaard op de harde schijf van het camerasysteem en daarna automatisch overschreven;
- De veiligheidscoördinator of een vestigingsdirecteur kan opdracht geven de beelden op een CD te branden;
- De veiligheidscoördinator bewaart deze beelden zolang hij nodig acht, echter niet langer dan één jaar. Dit in overleg met de vestigingsdirectie;
- De veiligheidscoördinator kan de CD ter beschikking stellen aan de politie. De politie dient daartoe de beelden schriftelijk te vorderen.

Het bekijken van de opgenomen beelden:

- Een bevoegde schoolfunctionaris mag bij het vermoeden van vandalisme, diefstal of een ander vergrijp de beelden bekijken om een mogelijke dader op te sporen. Deze kan de leerling of een collega toestemming geven mee te kijken;
- Bij een geweldsmisdrijf zal een bevoegde schoolfunctionaris de beelden bekijken om de mogelijke dader(s) te herkennen;
- In alle gevallen mogen de beelden alleen bekeken worden wanneer er een redelijke kans bestaat de mogelijke dader(s) te herkennen. Deze kan een slachtoffer of getuige toestemming geven om mee te kijken;
- Een bevoegde schoolfunctionaris is een medewerker die van de veiligheidscoördinator toestemming heeft de beelden te bekijken. Dit is Meinte Peterzon of Ivo Esser.
- De veiligheidscoördinator kan per incident anderen benoemen tot bevoegde schoolfunctionaris en deze toestemming geven de beelden zelfstandig te bekijken;
- De veiligheidscoördinator wordt altijd in kennis gesteld van wie de beelden heeft bekeken (leerling en/of medewerker) en wat het resultaat is geweest;
- De bevoegde schoolfunctionaris doet geen enkele mededeling, behalve aan de veiligheidscoördinator, vestigingsdirecteur of politie over datgene dat zichtbaar is op de beelden.

5. Het doen van aangifte op school

Bij diefstal of bij gebeurtenissen waar letsel en/of schade is toegebracht moet op het politiebureau aangifte gedaan worden. Wanneer de dader bekend is, wordt deze door de politie van school gehaald voor verhoor. Dit geeft in de school veel onrust. Vanuit het veiligheidsconvenant zijn werkafspraken gemaakt om in bepaalde gevallen aangifte op school op te nemen. Dit bevordert de rust op school. Ook wordt de totale tijdsduur erg ingekort, waardoor je meer een lik op stuk beleid krijgt, waardoor de dader(s) zich beter bewust worden van hun handelen. Wettelijke incidenten worden altijd geregistreerd in Magister.,

POLITIE
Noord-Holland Noord

Werkproces opnemen aangiftes in school:

1. De veiligheidscoördinator of schoolleider neemt contact op met de jeugdcoördinator bij de politie;
2. Een aangifte met aansluitend een verhoor van eventuele getuigen en een verhoor van de verdachte(n) wordt alleen opgenomen met de jeugdcoördinator bij de politie en/of de schoolcontactagent;
3. Voordat de politie naar school komt kan de verdachte leerling worden nagetrokken in het politie-informatiesysteem bps. Bekend is dan of het gaat om een first offender;
4. De leerjaarcoördinatoren/schoolleiders van de afdeling(en) waar de betrokken leerlingen inzitten, informeren vooraf de ouders;
5. De school verschaft gelegenheid en middelen om de verhoren discreet plaats te laten vinden binnen de school;
6. De politie neemt:
    - De aangifte;
    - De getuige verklaringen;
    - En de verdachte verklaringen meteen op.

6. Protocol (seksuele) intimidatie en (seksueel) geweld

- Het slachtoffer doet melding aan vertrouwenspersoon, docent of ander personeelslid van de school;
- De ontvanger van de melding luistert naar het slachtoffer. Stelt geen vragen. Maakt eventueel na het gesprek aantekeningen van wat gezegd is door het slachtoffer. (de ontvanger van de melding kan later als getuige gehoord worden);
- De ontvanger van de melding schakelt de vertrouwenspersoon van de school in en informeert de veiligheidscoördinator;
- De vertrouwenspersoon probeert het slachtoffer zover te krijgen dat hij/zij een vrijblijvend/vertrouwelijk gesprek wil aangaan met de zedenrechercheur van de politie;
- Als het slachtoffer een gesprek wil wordt een afspraak gemaakt door de vertrouwenspersoon;
- Indien het slachtoffer absoluut geen gesprek met de politie wil wordt er een melding gedaan aan het Advies- en Meldpunt Kindermishandeling;
- De veiligheidscoördinator doet altijd melding bij de politie i.v.m. mogelijke professionele opvang slachtoffer, sporenonderzoek en medisch onderzoek;
- De veiligheidscoördinator informeert de leerjaarcoördinator/schoolleider van de afdeling waarin het slachtoffer les volgt.

Wat moet nooit gedaan worden:

- Het slachtoffer uithoren over datgene wat er is gebeurd. Volsta met datgene wat het slachtoffer spontaan vertelt;
- Ga geen gesprekken aan met personen die door het slachtoffer eerder in vertrouwen zijn genomen (vrienden en vriendinnen e.d.);
- Deze handelingen kunnen namelijk in een later stadium een getuigenverklaring onbruikbaar maken. Bij twijfel kan er altijd overlegd worden met een zedenrechercheur.

Externe vertrouwenspersoon voor personeel

Indien je op de werkvloer te maken hebt met ongewenst gedrag kun je hiervoor terecht bij een vertrouwenspersoon. Binnen het Jan Arentsz zijn dit: Yvonne Siegel en Caroline van Eijck (vestiging Alkmaar) en Dorien de Graaf (vestiging Langedijk).

Daarnaast is er een externe vertrouwenspersoon die je kunt raadplegen: Praatuit.nl. Het Jan Arentsz heeft Praatuit.nl ingehuurd om collega's ondersteuning en een luisterend oor te bieden in het geval van ongewenst gedrag op de werkvloer. Zij zijn te bereiken via:
Whatsapp op 023-2010219 dit kan 24/7.
Ook kun je ons bellen op 023-2010219 tussen 9.00 en 21.00 uur of mailen naar info@praatuit.nl.

Of maak direct een afspraak voor ons online-spreekuur hier. Op naar een veilige werkvloer!
Praatuit Rijksstraatweg 165 2024 DE Haarlem T: 023 - 20 10 219 @: info@praatuit.nl Praatuit.nl

7. Spijbel- en verzuimbeleid

7a. Schematisch overzicht pedagogische richtlijnen VMBO Mandenmakerstraat

Laten we vooral ons gezond verstand (haarwater, onderbuik, intuïtie) gebruiken en onderstaande als richtlijn hanteren. Als we vinden dat we eerder moeten ingrijpen kan dat natuurlijk, maar later kan niet. Hieronder staan de maximale grenzen. Wekelijks krijgen de mentoren, schoolleiders en directie een overzicht van de absenties, te laat komen en verwijderingen van hun resp. klas, team en vestiging.
Bij contact met huis: steeds in telegramstijl in Magister onder contactregistratie noteren, als feitelijke informatie, dus zonder waardeoordeel.
Let op: bij een LGF-leerling moet ook de LGF-begeleider geïnformeerd worden.
Let op: inschakelen extern ZAT: mentor moet vooraf toestemming aan ouders vragen.

ABSENT

Gebeurtenis	Actie	Wie	Informatie aan
Absent zonder kennisgeving (oa)	Naar huis bellen voor 11.00 uur, bij geen gehoor: voicemail inspreken.	Meldkamer	
Leerling meldt zich tijdens schooldag ziek	Na contact met een ouder mag leerling vertrekken	Meldkamer	Mentor
Leerling is 3 achtereenvolgende schooldagen ziek	Naar huis bellen, met als insteek: belangstelling, zorg, geregeld m.b.t. schoolse zaken	Meldkamer informeert mentor over ziekte Mentor neemt contact op met huis	Indien nodig: vakdocenten en schoolleider
Leerling blijft ziek, is nu 5 schooldagen ziek	Opnieuw bellen	Meldkamer informeert mentor over ziekte Mentor neemt contact op met huis	Indien nodig: vakdocenten en schoolleider
Leerling is 40 lesuren (cumulatief) ziek	Geschiedenis bekijken, gegevens verzamelen	Meldkamer informeert mentor over ziekte Mentor neemt contact op met huis	Schoolleider Indien nodig: intern ZAT

ONGEOORLOOFD ABSENT

Gebeurtenis	Actie	Wie	Informatie aan
Ongeoorloofd absent	Controleren en bij twijfel naar huis bellen Indien ongeoorloofd absent: afhandelen als spijbelen, dus z.s.m. dubbel terug laten komen	Meldkamer	Brief aan ouders, mailtje aan mentor en schoolleider
Onderbouw: v/a 2 uur spijbelen	Afhandelen als spijbelen, dus z.s.m.	Meldkamer signaleert, informeert schoolleider	Mentor, schoolleider en zoco

Bovenbouw: v/a 4 uur spijbelen ('met voorbedachten rade') of meer dan 1 dag	dubbel terug laten komen Melden via DUO bij leerplicht Gesprek met leerling Ouders informeren	Schoolleider meldt bij DUO[1] Meldkamer Mentor Mentor	Schoolleider, indien nodig intern/extern ZAT

De school is verplicht te melden via DUO na 3 achtereenvolgende verzuimdagen of na 16 lessen in 4 achtereenvolgende weken. Wij willen eerder melden.

TE LAAT

Gebeurtenis	Actie	Wie	Informatie aan
3x te laat	3x vroeg melden in G09 Brief naar huis	Meldkamer Meldkamer	Mentor en schoolleider
5x te laat	5x vroeg melden Brief naar huis Bellen naar huis	Meldkamer Meldkamer Mentor	Mentor en schoolleider Evt. intern ZAT
8x te laat	Brief naar huis Bellen naar huis[2] Bespreken in intern ZAT	Meldkamer Mentor Mentor	Mentor en schoolleider Intern ZAT
11x te laat	Brief naar huis Kopie van deze brief naar leerplicht Eventueel extern ZAT	Meldkamer Meldkamer Mentor	Mentor en schoolleider Leerplicht kopie van brief Eventueel extern ZAT
15x te laat	Brief naar huis Melden in DUO	Meldkamer Schoolleider	Mentor en schoolleider en zoco

Iedere dag is G08 van 7.45 – 8.45 als meldkamer geopend. Als een leerling zich vroeg moet melden, is dat ook in G08.

VERWIJDERD, bij extreme zaken altijd overleg met zoco en/of directie en/of schoolleider

Gebeurtenis	Actie	Wie	Informatie aan
1x verwijderd	Leerling vult formulier in Spreken met leerling	Meldkamer Docent (en mentor)	Docent, mentor en schoolleider
2x of 3x verwijderd	Leerling vult formulier in Bellen naar huis	Meldkamer Mentor	Docent, mentor en schoolleider
3x tot 5x verwijderd	Leerling vult formulier in	Meldkamer Mentor	Docent, mentor en schoolleider

[1] afwezigheid bij plusuur: niet direct de eerste keer bij DUO melden, wel bij structurele afwezigheid plusuur.

[2] melden dat bij voortduring leerplichtambtenaar en/of ZAT wordt geïnformeerd.

	Gesprek met ouders, gemaakte afspraken bevestigen per brief naar huis Interne /externe schorsing overwegen	Schoolleider, na raadpleging zoco en/of directie	
6x verwijderd	Leerling vult formulier in Bespreken in intern ZAT Interne /externe schorsing overwegen	Meldkamer Mentor Schoolleider, na raadpleging zoco en/of directie	Docent, mentor en schoolleider
2x verwijderd op 1 dag	Leerling zit tot 16.00 uur in de meldkamer Bellen en brief naar huis	Meldkamer Meldkamer	Docent, mentor en schoolleider

7b. Schematisch overzicht pedagogische richtlijnen HAG Mandenmakerstraat

Laten we vooral ons gezond verstand (onderbuik, intuïtie) gebruiken en onderstaande als richtlijn hanteren. Als we vinden dat we eerder moeten ingrijpen kan dat natuurlijk, maar later kan niet. Hieronder staan de maximale grenzen. Periodiek krijgen de mentoren en schoolleiders een overzicht van de absenties, te laat komen en verwijderingen van hun resp. klas, team en vestiging.

Bij contact met huis: steeds in telegramstijl in Magister onder contactregistratie noteren, als feitelijke informatie, dus zonder waardeoordeel.
Let op: bij een LGF-leerling moet ook de LGF-begeleider geïnformeerd worden.
Let op: inschakelen extern ZAT: mentor moet vooraf toestemming aan ouders vragen.

ABSENT

Gebeurtenis	Actie	Wie	Informatie aan
Absent zonder kennisgeving (oa)	Naar huis bellen voor 11.00 uur, bij geen gehoor: voicemail inspreken.	Meldkamer	
Leerling meldt zich tijdens schooldag ziek	Na contact met een ouder mag leerling vertrekken	Meldkamer	
Leerling is 4 achtereenvolgende schooldagen ziek	Naar huis bellen, met als insteek: belangstelling, zorg, geregeld m.b.t. schoolse zaken	Meldkamer informeert mentor over ziekte Mentor neemt contact op met huis	Indien nodig: vakdocenten en schoolleider
Leerling is 40 lesuren (cumulatief) ziek	Geschiedenis bekijken, gegevens verzamelen	Meldkamer informeert mentor over ziekte Mentor neemt contact op met huis	Schoolleider Indien nodig: intern ZAT

ONGEOORLOOFD ABSENT

Gebeurtenis	Actie	Wie	Informatie aan
Ongeoorloofd absent	Controleren en bij twijfel naar huis bellen Indien ongeoorloofd absent: afhandelen als spijbelen, dus z.s.m. dubbel terug laten komen		Mailtje aan mentor en schoolleider. Bij herhaling verzuimspreekuur.
16 uur ongeoorloofd absent in 4 weken.	Melden bij DUO. Gesprek met leerling en ouders.	Meldkamer signaleert en meldt bij DUO. Schoolleider.	Mentor, schoolleider en zorgcoördinator.

De school is verplicht te melden via DUO na 3 achtereenvolgende verzuimdagen of na 16 lessen in 4 achtereenvolgende weken. Wij willen eerder melden.

TE LAAT

Gebeurtenis	Actie	Wie	Informatie aan
3x te laat	3x vroeg melden	Meldkamer	Mentor en schoolleider
7x te laat	7x vroeg melden Brief naar huis	Meldkamer Meldkamer	Mentor en schoolleider
10x te laat	Brief naar huis Kopie van deze brief naar leerplicht	Meldkamer Meldkamer	Mentor en schoolleider Leerplicht kopie van brief
15x te laat	Brief naar huis Melden in DUO	Meldkamer Schoolleider	Mentor en schoolleider en zoco

Opmerking: Periodiek houdt de leerplichtambtenaar verzuimspreekuren

VERWIJDERD, bij extreme zaken altijd overleg met zoco en/of directie en/of schoolleider

Gebeurtenis	Actie	Wie	Informatie aan
1x verwijderd	Leerling vult formulier in Spreken met leerling	Meldkamer Docent (en mentor)	Docent, mentor en schoolleider
3x tot 5x verwijderd	Leerling vult formulier in Gesprek schoolleider met leerling, gemaakte afspraken bevestigen per brief naar huis Interne /externe schorsing overwegen	Meldkamer Schoolleider, na raadpleging zoco en/of directie	Docent, mentor en schoolleider
6x verwijderd	Leerling vult formulier in Interne /externe schorsing overwegen	Meldkamer Mentor Schoolleider, na raadpleging zoco en/of directie	Docent, mentor en schoolleider

7c. Verzuimbeleid vestiging Langedijk

Jan Arentsz, vestiging Langedijk

1. Verzuimregistratie

Beschrijving	**actie**
1.1. Invoer in Magister van telefonische meldingen die binnenkomen via de conciërge of meldkamer	Invoer door VZC
1.2. Invoer in Magister van verzuimkaarten die via blauwe brievenbus zijn ingeleverd.	Invoer door VZC
1.3 Invoer in Magister van verlofaanvragen die door leerjaarcoördinator akkoord zijn verklaard.	Info van LJC naar VZC Invoer door VZC
1.4 Ieder lesuur controle van aanwezigheid van leerlingen in alle klassen en vergelijken met dat wat al bekend was. In het 1e/2e lesuur vd leerling wordt er naar huis gebeld. Bij absenties in andere lesuren wordt een mail naar ouders gezonden	Controle en bellen door VZC
1.5. Invoer in Magister van absenties gemeld via email en absentiekaart absentiekaart	Invoer door VZC

2. Soorten verzuim

beschrijving	**actie**
2.1 Ongeoorloofd verzuim – absoluut verzuim Hiervan is sprake als een leerplichtige jongere niet ingeschreven staat bij een school of onderwijsinstelling. De school meldt binnen zeven dagen de in- of uitschrijving, opdat de leerplichtambtenaar (RMC) kan controleren of de jongere al dan niet onderwijs volgt.	Melding door LLADM
2.2 Ongeoorloofd verzuim – luxe verzuim Hiervan is sprake als een leerplichtige jongere zonder toestemming wegblijft vanwege extra vakantie of familiebezoek. De verzuimcoördinator geeft dit door aan de leerjaarcoördinator. De ljc geeft VZC opdracht een DUO-melding te doen. Is een verzoek tot extra vakantieverlof niet akkoord, dan houdt de verzuimcoördinator in de gaten of het verlof door de ouders op een andere wijze alsnog wordt genomen. Is dat het geval dan licht de verzuimcoördinator de leerjaarcoördinator in.	VZC geeft verzuim door aan LJC. LJC laat LLADM melding doen. VZC houdt afgewezen verlof in de gaten VZC informeert LJC
2.3 Ongeoorloofd verzuim - relatief verzuim - spijbelen Hiervan is sprake als een leerplichtige jongere wel op een school staat ingeschreven, maar zich onttrekt aan regels van de aanwezigheidsplicht, zoals bijvoorbeeld spijbelen. Spijbelen geeft de VZC via het digitale verzuimloket aan de leerplichtambtenaar door. De coördinator belt de ouders (wanneer de VZC nog geen contact heeft gehad) of kiest ervoor om hen een brief te sturen. a. Een leerling spijbelt voor de eerste maal een of twee lesuren. b. Een leerling spijbelt opnieuw en/of spijbelt meer dan twee lesuren. c. Bij herhaling van spijbelen volgt een schorsing, mits er naar het oordeel van de leerjaarcoördinator reden is dit niet te doen.	VZC doet melding en maakt melding in leerlingvolgsysteem. Indien VZC de ouders nog niet heeft geïnformeerd, doet de LJC dit. VZC geeft spijbelaar aan LJC door VZC laat gespijbelde tijd 2 x 60 minuten inhalen VZC geeft spijbelen door aan LJC.

	LJC laat gespijbelde tijd 2x 60 minuten inhalen LJC laat VZC melding doen. LJC schorst de leerling, mits …
2.4 Ongeoorloofd verzuim – relatief verzuim - te laat komen a. wanneer een leerling te laat op school is, komt deze in dezelfde week een half uur terug. b. wanneer op vrijdag blijkt dat de leerling dit niet heeft gedaan, mailt de verzuimcoördinator een brief naar de ouders: de leerling komt op de in de brief genoemde datum een uur terug. c. komt de leerling dan nog niet terug, dan volgt een schorsing. d. het hele schooljaar checkt de VZC wie > 5 keer te laat is geweest. Bij >5 keer te laat wordt de leerling voorgedragen voor een gesprek met de LPA Langedijk. Deze komt ca. 4 keer per jaar naar JA Langedijk De leerplichtambtenaar voert dit gesprek ook voor leerlingen van andere gemeenten en geeft de informatie dan aan de collega door. De VZC maakt een melding van dit gesprek in het magisterlogboek. e. Komt een leerling voor de twaalfde maal te laat, dan stuurt de VZC een email naar de leerplichtambtenaar. De LPA regelt een HALT-straf. De ljc geeft opdracht aan VZC tot het maken van een DUO-melding f. vervallen	VZC controleert terugkomen leerling VZC mailt brief aan ouders VZC geeft door aan LJC LJC schorst de leerling VZC stuurt email naar leerplichtambtenaar VZC noteert leerlingen voor het spreekuur VZC informeert LPA. LPA regelt HALT-straf
2.5 Geoorloofd verzuim (Langdurig) ziekteverzuim en verzuim op basis lichamelijke en/of psychische klachten waarbij de reden van het verzuim is nog onvoldoende duidelijk is. Schoolverzuim door leerlingen met lichamelijke en/of psychische klachten vraagt om een heldere signalering door deskundigen. Op schoolniveau betekent dit een nauwe samenwerking tussen de mentor, de leerjaarcoördinator, het zorgadviesteam (ZAT), Jeugdzorg, schoolmaatschappelijk Werk, de leerlingenbegeleider en de leerplichtambtenaar. Het doel is de leerling door te verwijzen naar de juiste hulpverlening. a. De mentor en VZC houden het eerste zicht op zijn of haar leerlingen en neemt contact op met de ouders wanneer de leerling meer dan een week afwezig is.	VZC informeert LJC over afdeling. VZC informeert mentor. Mentor spreekt met de leerling en belt de ouders. Mentor belt ouders

b. Als een leerling 50 lesuren heeft verzuimd, belt de mentor de ouders om hen te wijzen op de ernst van en de eventuele gevolgen van het verzuim. c. Bij > 70 uren verzuim tipt de VZC de LJC. De LJC neemt contact op met de ouders. Bij > 90 uren verzuim idem. LJC besluit wel/niet een DUO-melding te doen. Indien besloten wordt tot DUO-melding geeft LJC de VZC daartoe opdracht. d. Voor a t/m c geldt dat we, hoewel de ouders de afwezigheid steeds hebben gemeld, bij twijfel over kunnen gaan op een melding bij de leerplichtambtenaar of zelfs een AMK-melding. De leerjaarcoördinator brengt de ouders van dit voornemen schriftelijk op de hoogte.	LJC gesprek met ouders. LJC oordeelt over rechtmatigheid verzuim. LJC schrijft ouders een brief.
2.6 Aangevraagd verlof De leerjaarcoördinator toetst een aanvraag van de ouders/verzorgers aan de leerplichtwet. Eventueel heeft de leerjaarcoördinator overleg met de school waarop ook nog een ander kind van hetzelfde gezin zit.	LJC verleent verlof of wijst af. LJC overleg soms met andere school.
2.7 Signaalverzuim (zowel geoorloofd als ongeoorloofd) Verzuim is vaak een uitvloeisel van een achterliggende problematiek. Is dat het geval, dan spreken we ook wel van 'zorgwekkend verzuim' of 'signaalverzuim'. Dit is het geval als het verzuim een signaal is voor problemen als: ● leerproblemen, leerstoornissen; ● sociaal-emotionele problemen of stoornissen; ● (ernstige) gedragsproblemen of gedragsstoornissen; ● gezondheidsproblemen (fysiek en psychisch/psychiatrisch; wordt vaak gemeld als ziekteverzuim); Ter beoordeling van de leerjaarcoördinatoren volgen we daarin de stappen van geoorloofd of ongeoorloofd verzuim. Het oordeel van de zorgcoördinator en de leerlingbegeleider kunnen daarin een rol spelen.	Ter beoordeling van LJC

3 Communiceren van verzuimbeleid

Delen van het verzuimbeleid dienen duidelijk in- en extern gecommuniceerd te worden. Dat betekent dat de procedures helder moeten zijn en dat we de leerlingen en ouders van de belangrijkste feiten op de hoogte brengen. Alle procedures rondom verzuim staan helder vermeld op de website van JA-Langedijk.

4 Leerplichtambtenaar

4.1 Kerntaken
De opdracht van de leerplichtambtenaar is het tegengaan van schoolverzuim en voortijdig schoolverlaten (VSV).
De kerntaken zijn:

- Preventief controleren en adviseren;
- Toezicht houden op naleving van de Leerplichtwet/kwalificatieplicht;

- Verwijzen naar (jeugd)hulpverlening;
- (Bevorderen) de samenwerking met alle bij een leerling betrokken partijen;
- Handhaven en sanctioneren.

De leerplichtambtenaar heeft een te-laat-kom spreekuur op school. De LPA Langedijk heeft contact met de LPA van de gemeente waar de leerling woont.

4.2 Strafoplegging

Voor beginnende spijbelaars zonder ernstige achterliggende problematiek kan een Halt Proces Verbaal worden opgemaakt. Dat kan alleen als er dit schooljaar niet eerder een Halt-afdoening heeft plaatsgevonden.

Bij aanhoudend verzuim waarbij eerdere interventies geen resultaat hebben gehad kan een justitieel Proces Verbaal worden opgemaakt. Dat kan tegen ouders en/of de jongere vanaf 12 jaar. Bij een justitieel Proces Verbaal tegen de jongere wordt altijd een Raadsonderzoek gestart.

In het geval van luxe verzuim:

- bij 1 dag krijgen de ouders een waarschuwingsbrief;
- bij 2 dagen volgt een uitnodiging voor een gesprek bij de leerplichtambtenaar;
- bij 3 dagen of meer wordt een Proces Verbaal opgemaakt;
- bij herhaling wordt altijd een Proces Verbaal opgemaakt.

8. Handelingsprotocol bij ongewenst bezoek op het schoolterrein

De ongewenste persoon is bij de school bekend:

- Twee personeelsleden verzoeken de ongewenste persoon zich te verwijderen;
- Bij weigering wordt de ongewenste persoon gesommeerd te vertrekken;
- Bij weigering wordt deze sommering herhaald met de toevoeging dat anders de politie wordt gebeld;
- Bij weigering politie bellen;
- Overleg tussen de contactpersonen van de school en de politie;
- Indien ongewenst persoon terugkomt: wederom het zelfde protocol hanteren.

De dader is bij de school niet bekend (zie hiervoor ook het protocol ongewenst bezoek op het schoolterrein):

- Wanneer er een melding binnenkomt zo veel mogelijk informatie vragen. Alle informatie noteren. Ook de naam van de melder noteren en na afloop terugkoppelen wat er gedaan is;
- Noteer datum en tijdstip van de melding;
- Altijd met een ander (conciërge, schoolleiding lid of veiligheidscoördinator) gaan naar de plaats waar het probleem zich voordoet. Telefoon meenemen;
- Afspreken wie eventueel het (auto)nummer en signalement noteert en wie het woord voert;
- Wees in eerste instantie vriendelijk. Vraag eerst wat er aan de hand is. Vraag dan vriendelijk om te vertrekken, omdat het privé terrein is. Zeg dan opnieuw dat het privé terrein is en sommeer daarna om te vertrekken. Ga niet in discussie;
- Ga bij brutaliteit niet in discussie, maar loop rustig weg;
- Bel buiten zicht de politie en verwijs naar het convenant dat we hebben en noteer ook weer het tijdstip. Noteer ook wat er gezegd is;
- Politie opvangen en alle informatie doorgeven;
- Wanneer de politie niet komt eventueel achtergebleven sporen verzamelen. Raak hierbij niets met je handen aan (vingerafdrukken, gevaar voor AIDS) maar verzamel spullen met een pincet en doe alles in een plastic opbergzakje. Op het zakje datum en tijdstip noteren. Of vraag de veiligheidscoördinator dit te doen;
- Geef meteen na het gebeuren ook alle informatie en spullen aan de veiligheidscoördinator en/of vul het formulier in.

9. Zorgvuldig omgaan met informatie en social media

Vanwege het specifieke karakter (het grote bereik) van de social media is de bijlage opgedeeld in een algemeen deel, betreffende alle vastlegging van (persoons)informatie en een specifiek deel, betreffende social media.

Bewust 6x zorgvuldig omgaan met informatie
Als je persoonsgegevens deelt met anderen, dan moet je er op kunnen vertrouwen dat de ontvanger zorgvuldig met jouw gegevens omgaat. Als je werk met persoonsgegevens vraagt dit dan ook van medewerkers en leerlingen een aantal basisvaardigheden rondom het gebruiken en delen van persoonsgegevens. Dit vatten we samen als 'Bewust 6x Zorgvuldig'.

1. **Gebruik zorgvuldig: vergrendel je scherm**
   Verlaat je je werkplek om koffie te halen of wat anders, vergrendel je scherm. Niet alle informatie is voor iedereen bestemd. Windows-toets L vergrendelt direct je pc. Beveilig ook je privé PC met wachtwoord en virusscanner. Zorg dat je mobiele telefoon is voorzien van een toegangscode.

2. **Deel zorgvuldig: eerst denken, dan delen**
   Stel jezelf bewust de vraag welke gegevens ga ik delen, is dat niet te veel, kan het met minder gegevens. Zijn er alternatieven. Met wie deel ik de gegevens, mogen zij alles hebben. Gebruik het BCC veld bij een mail naar meerdere personen, groepen, organisaties. Vermijd discussies met leerlingen, ouders/verzorgers of derden op digitale media (nodig ze zo nodig uit voor een persoonlijk gesprek). Wees alert op wat je deelt in Whatsapp-groepen met je leerlingen mocht je daarvan gebruik maken. Welke afspraken zijn er voor Whatsapp groepen?

3. **Surf zorgvuldig: klik niet klakkeloos**
   Denk vooraf goed na voor je klikt op een link in de mail of op een website, wees je bewust van eventuele gevaren als *ransomware* enz.

4. **Beveilig zorgvuldig: je wachtwoord is persoonlijk, deze leen je dus niet uit**
   - Kies alleen hele goede (tips: https://www.seniorweb.nl/tip/tip-maak-een-sterk-wachtwoord)
   - Vervang ze regelmatig.
   - Bewaar ze op een veilige plek.
   - Geef ze nooit aan iemand anders.

5. **Verbind zorgvuldig: check veilige verbinding**
   Vermijd gratis wifi mogelijkheden, check veilige verbindingen in de browser (o.a. groen slotje).
   School voorziet in de juiste gegevenstoegang om veilig met persoonsgegevens te werken.

6. **Sla zorgvuldig op**
   Gebruik bij voorkeur de toegestane cloud-opslag (Microsoft 365).

Zorgvuldig omgaan met social media

Wij besteden op school aandacht aan het leren omgaan met social media en leggen daarbij het verband met de bedoeling van ons onderwijs. Er is structureel aandacht voor het gebruik van social media in de lessen informatiekunde, projecten en in situaties waarin conflicten zijn die te maken hebben met social media.

Bij gebruik van social media zijn privé-gerelateerde en werk gerelateerde zaken niet zo gemakkelijk te scheiden. Medewerkers van Csg Jan Arentsz mogen actief zijn op social media mits het werk er niet onder lijdt. Het uitgangspunt bij het gebruik van social media door medewerkers is dat zij hiermee verstandig omgaan. Het gedrag op social media wijkt niet af van het levensechte gedrag binnen Csg Jan Arentsz.

Deze richtlijnen hebben te maken met situaties waarbij er een overlap is (of kan zijn) tussen werk en privé. Weblogs, fora en netwerken waar je alleen als privépersoon actief bent – over activiteiten die geen raakvlak hebben met de werksituatie – vallen hier expliciet niet onder.

Richtlijnen gebruik social media

1. Medewerkers proberen kennis en andere waardevolle informatie te delen, mits die informatie niet vertrouwelijk is en Csg Jan Arentsz niet schaadt.
2. Medewerkers kunnen zich mengen in discussies op social media over onderwijszaken. Dit kan op basis van persoonlijke ervaringen. Als een standpunt van Csg Jan Arentsz gepubliceerd wordt, vermeldt de schrijver dit.
3. Voor het publiceren van gesprekken, foto's, filmpjes wordt eerst expliciete schriftelijke toestemming gevraagd aan de betrokkenen (of ouders/voogd). Deze toestemming dient te worden bewaard in het personeelsdossier of leerlingdossier van betrokkenen;
4. Bij onderwijs-onderwerpen maken medewerkers duidelijk dat zij op persoonlijke titel publiceren, tenzij dit met toestemming van de schoolleiding gebeurt.
5. Medewerkers van Csg Jan Arentsz gaan niet in discussie met een leerling, ouder/verzorger of derde op social media of andere digitale media. Mocht er aanleiding toe bestaan wordt deze persoon uitgenodigd voor een gesprek. Wanneer een online discussie dreigt te ontsporen, of in het ergste geval al helemaal ontspoord is, neem dan direct contact op met de verantwoordelijke afdeling/persoon en overleg over de te volgen strategie
6. Wees je, als medewerker van Csg Jan Arentsz, bewust van het feit dat er al snel een relatie gelegd kan worden met je werkzaamheden voor de school – ook als je een privé mening verkondigt.
7. Medewerkers van Csg Jan Arentsz zijn persoonlijk verantwoordelijk voor wat zij publiceren.
8. Medewerkers van Csg Jan Arentsz zijn zich ervan bewust dat publicaties op social media altijd vindbaar zijn.
9. Bij twijfel over een publicatie overleggen medewerkers met collega's of leidinggevende.
10. Csg Jan Arentsz zorgt ook digitaal voor een veilig klimaat en het gedrag van medewerkers op social media wijkt niet af van wat in de klas en op school gebruikelijk is.
11. Leerlingen die op social media het veilige klimaat op Csg Jan Arentsz 'in gevaar' brengen worden daarop aangesproken.
12. In lessen wordt aandacht besteed aan het gebruik van social media door leerlingen en indien er een aanleiding toe is wordt er extra aandacht aan besteed.
13. Csg Jan Arentsz neemt bij overtreding van digitale omgangsvormen dezelfde maatregelen als bij overtreding van mondelinge of schriftelijke omgangsvormen.

Veiligheid

Csg Jan Arentsz heeft een verantwoordelijkheid als het gaat om de veiligheid van leerlingen en personeel. Dat begint met duidelijke en gecommuniceerde normen en waarden en de handhaving daarvan, ook digitaal. Daarom hanteert Csg Jan Arentsz duidelijke regels over het gebruik van computer devices

- Computer devices zijn niet meer weg te denken in de huidige maatschappij en daarom toegestaan op school;
- Computer devices dienen uit te staan tijdens de lessen tenzij de docent heeft aangegeven dat de computer devicer tijdens de les mag worden gebruikt;
- De schoolbrede afspraak rondom telefoons is: de leerling heeft de mobiele telefoon in de kluis of in de telefoontas in het lokaal tijdens de lessen. Het is niet toegestaan dat een leerlingen de telefoon in de lessen bij zich draagt. Gebeurt dit wel, dan kan de docent de telefoon innemen. Aan het einde van de lesdag kan de leerling de telefoon ophalen bij een vast punt in de vestiging.
- Uitzonderingen worden individueel in overleg met de schoolleiding bepaald
- Aan leerlingen die computer devices ongeoorloofd gebruiken en/of zich norm overschrijdend gedragen zullen de gebruikelijke sancties (zie leerlingenstatuut en schoolreglement) worden opgelegd;
- Bij ongeoorloofd gebruik of norm overschrijdend gedrag worden de ouders/ vertegenwoordigers ingelicht. Gedacht kan worden aan kleineren van medewerkers of leerlingen via YouTube, dreigtweets, digitaal pesten en/of seksuele intimidatie;
- De schoolleider bepaalt wanneer het norm overschrijdend gedrag zodanig is dat de politie dient te worden ingeschakeld. Dit gebeurt in ieder geval als er sprake is van bedreiging.
- Bij ongeoorloofd of norm overschrijdend gedrag wordt de veiligheidscoördinator op de hoogte gebracht.
- Als er sprake is van aanwijsbare slachtoffers van eventueel norm overschrijdend gedrag wordt hen zo nodig hulp aangeboden;
- Als het norm overschrijdend gedrag leidt tot media-aandacht wordt de pers door de betreffende vestigingsdirecteur of, in geval van ernstige incidenten, de voorzitter college van bestuur te woord gestaan.

10. Procedure melding datalekken

Inleiding
Onze school is verplicht om datalekken in of hacks van systemen te melden.
Datalekken moeten gemeld worden bij de Autoriteit Persoonsgegevens in de volgende gevallen:

- Als een datalek is geconstateerd in een geautomatiseerd gegevensbestand waarvoor Csg Jan Arentsz verantwoordelijk is en wat gegevens bevat die tot een persoon (leerling, ouder/verzorger, medewerker of ander, aan school gerelateerd persoon) herleidbaar zijn.
- Bij verlies en/of ongeautoriseerde toegang tot een informatie systeem/computer device (zoals: laptop, mobiele telefoon, etc) dat gegevens bevat die tot een persoon (leerling, ouder/verzorger, medewerker of ander, aan school gerelateerd persoon) herleidbaar zijn.
- Indien er sprake is van een inbreuk op de beveiliging van persoonsgegevens die leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens.

NB: Als het datalek of de hack gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n), moet het ook aan hen gemeld worden.

De rol van externe partijen
Veel van de persoonsgegevens worden door medewerkers in de schoolomgeving geregistreerd en bewaard. Een groot deel van de registratie vindt echter bij externe leveranciers plaats. Deze leveranciers zijn schriftelijk op de hoogte gesteld van hun verplichting om een mogelijk lekken van data m.b.t. Csg Jan Arentsz direct na constatering te melden bij de applicatiebeheerder.

Bronsystemen bij externe partijen waarvan datalekken binnen 2 werkdagen gemeld moeten worden aan de Autoriteit persoonsgegevens zijn:

a. Leerlingadministratiesysteem Magister, inclusief:
    I. Facet – digitale toetsing voor Rekentoetsen, CSPE's, DTT-pilot en CE's in VMBO
    II. OSO – beveiligde uitwisseling leerlingendossiers tussen PO en VO
    III. TOPdossier, wordt binnenkort ingevoerd t.b.v. beveiligde informatie-overdracht zorgleerlingen.
b. Elektronische leeromgeving Moodle
c. Personeelsadministratiesysteem AFAS
d. Databases van uitgevers waarin leerlinginformatie is opgeslagen

Andere informatiesystemen bij externe partijen die mogelijk datalekken kunnen veroorzaken of daar debet aan kunnen zijn:

e. Entree-koppelingen (ook naar de methodensites) vanuit Magister of Moodle
f. Microsoft Active Directory-koppelingen en Google Suite for Education-koppelingen
g. Bookmaster, het registratiesysteem van de boeken-/licentieleverancier

Signalering, melding en escalatie van datalekken

- Signalering van datalekken is belegd bij de functioneel beheerders van de systemen. Dit zijn de personen die bij uitstek als een van de eersten op de hoogte zijn van een mogelijk datalek in zo'n systeem.
- Ook alle andere medewerkers die gebruik maken van gegevensdragers zijn verplicht om een datalek in hun gegevensdrager te melden.
- Bij de signalering van een datalek meldt de functioneel beheerder (of de medewerker die het betreft) dit direct bij de veiligheidscoördinator. Tevens registreert de functioneel beheerder het datalek in het incidentenregistratiesysteem van Magister
- De veiligheidscoördinator verricht een beoordeling conform de eisen van de wet- en regelgeving (Algemene verordening gegevensbescherming).
- De veiligheidscoördinator bespreekt de beoordeling met het bevoegd gezag (voorzitter CvB).
- Als het datalek valt in de categorieën zoals in de inleiding gesteld meldt de veiligheidscoördinator dit namens het bevoegd gezag bij de Autoriteit persoonsgegevens. Dit gebeurt via het digitale meldloket van de autoriteit persoonsgegevens.
- Als het datalek of de hack gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n), meldt de veiligheidscoördinator dit ook aan hen.
- De veiligheidscoördinator vult de melding in het incidentenregistratiesysteem aan met de ondernomen acties.

11. Informatiebeveiliging en privacybeleid

1. Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ICT. Deze afhankelijkheid van ICT en gegevensvastleggingen brengt nieuwe kwetsbaarheden en risico's met zich mee.
Het doel van dit Informatie Beveiliging en Privacy Beleid is dat we als Csg Jan Arentsz een (digitale) omgeving hebben waar veilig wordt omgegaan met informatie en privacy is gewaarborgd.
Een afgeleid doel is dat we voldoen aan de wet- en regelgeving, zoals de Algemene verordening gegevensbescherming en dat zichtbaar kunnen maken voor accountant en inspectie.
Met de beschreven maatregelen willen we risico's tot een aanvaardbaar niveau reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal kunnen waarborgen.

1.1. *Toelichting informatiebeveiliging*

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de vertrouwelijkheid en kwaliteit van de informatievoorziening te garanderen.
Hierbij gaat het om:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten;
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn;
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan er toe leiden dat informatie in handen van onbevoegden komt. Incidenten en inbreuken op de informatiebeveiliging kunnen leiden tot financiële schade en imagoverlies.

1.2. *Toelichting privacy*

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen veilig te worden bewaard. Daartoe is wet – en regelgeving opgesteld. Deze regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn alle gegevens die herleidbaar zijn tot een individu. Onder verwerking wordt verstaan elke handeling met betrekking tot die persoonsgegevens. De wet noemt als voorbeelden van verwerking: *het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.*

1.3. Vervlechting informatiebeveiliging en privacy

Informatiebeveiliging en een zorgvuldige omgang met persoonsgegevens zijn belangrijke voorwaarden voor het kunnen garanderen van privacy. Informatiebeveiliging en privacy staan naast elkaar, en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Het hier beschreven beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen Csg Jan Arentsz.

2. Doel en reikwijdte

2.1. Doel

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van de informatievoorziening in het onderwijs en de bedrijfsvoering van Csg Jan Arentsz.
- Het garanderen van de privacy van leerlingen en medewerkers van Csg Jan Arentsz waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkenen wordt gerespecteerd en Csg Jan Arentsz voldoet aan relevante wet- en regelgeving.

2.2. Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen Csg Jan Arentsz geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden. Dus ook privé-apparatuur van waaruit toegang tot het schoolnetwerk wordt gezocht.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van Csg Jan Arentsz. Het beleid heeft betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites, waarbij de betreffende persoon die de informatie verspreid uitdrukkelijk een eigen verantwoordelijkheid heeft.
- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Csg Jan Arentsz waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan Csg Jan Arentsz persoonsgegevens verwerkt.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van Csg Jan Arentsz evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- IBP-beleid binnen Csg Jan Arentsz heeft raakvlakken met:
  - Algemeen veiligheidsbeleid (zie Veiligheidsbeleidsplan); met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
  - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties (zie HR-processen)
  - IT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen, waarbij wij aansluiten op de landelijk gehanteerde standaarden van Kennisnet;
  - Medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers

- Beleid inzake aanschaf en gebruik van ICT en digitale leermiddelen.

3. Uitgangspunten

3.1. Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Csg Jan Arentsz zijn:

- Informatiebeveiliging en privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking treedt). De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans noodzakelijk is tussen het belang van Csg Jan Arentsz om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens .
- Binnen Csg Jan Arentsz is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten.
- De school is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden geïnformeerd over de regelgeving rond het gebruik van informatie.
- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij Csg Jan Arentsz geclassificeerd.
- De classificatie is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik gemaakt wordt van de classificatie. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- Csg Jan Arentsz sluit met alle leveranciers van (digitale) onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Csg Jan Arentsz heeft hiervoor een protocol "zorgvuldig omgaan met informatie en social media" geformuleerd, vastgesteld en geïmplementeerd.
- Informatiebeveiliging en privacy is bij Csg Jan Arentsz een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie-)systemen, wordt bij Csg Jan Arentsz vanaf de start rekening gehouden met informatiebeveiliging en privacy.

3.2. *Uitgangspunten privacy*

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij Csg Jan Arentsz zijn:

1. **Doelbepaling en doelbinding**: Persoonsgegevens worden alleen verzameld met een vooraf vastgesteld en concreet doel. Deze persoonsgegevens mogen alleen worden verwerkt omdat vastgestelde doel te bereiken.

2. **Grondslag**: Verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie**: De persoonsgegevens die de school verwerkt, zijn redelijkerwijs nodig om het doel te bereiken. De gegevens staan in verhouding tot het doel ('proportioneel') en het doel kan niet met minder dan deze verzamelde gegevens worden bereikt ('subsidiair').
   Het gaat er dus om dat de school uitsluitend gegevens verzamelt die écht nodig zijn om het doel te bereiken. Niet: zo min mogelijk gegevens, wel: alleen relevante gegevens. Dataminimalisatie heeft ook te maken met bewaartermijnen en nog meer met het vernietigen van data als het bewaartermijn is verstreken.
4. **Transparantie**: De betrokkene (dus: de leerling en/of zijn ouders) is in begrijpelijke taal geïnformeerd over wat er aan informatie wordt verwerkt en wat het doel daarvan is. De leerling en zijn ouders zijn op de hoogte van hun rechten als het gaat om de verwerking van persoonsgegevens door de school.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.

Persoonsgegevens worden adequaat beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van toestemming, zal Csg Jan Arentsz aan de betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

4. **Wet- en regelgeving**

Bij Csg Jan Arentsz voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

5. **Organisatie**

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol.
Dit hoofdstuk beschrijft hoe IBP in Csg Jan Arentsz is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben, bij welke functies de rollen zijn ondergebracht en wat de documenten zijn die daarbij passen.

5.1. *Rollen (functies) rondom IBP*

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken wordt bij Csg Jan Arentsz een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

5.1.1. *Richtinggevend*

Eindverantwoordelijke

Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.

5.1.2. *Sturend*

Werkgroep IBP Normenkader

Adviseert het College van Bestuur/directeur bedrijfsvoering en is mede verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen Csg Jan Arentsz.
De IBP werkgroep vertaalt het beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling en zorgt ervoor dat het Jan Arentsz voldoet aan het IBP normen kader voor VO.

Functionaris voor Gegevensbescherming (Bij Csg Jan Arentsz belegd bij de veiligheids coordinator (Hoofd FacZ))

Hij houdt binnen Csg Jan Arentsz toezicht op de toepassing en naleving van de AVG. De veiligheidscoordinator zorgt voor het afhandelen van vertrouwelijke (informatiebeveiligings)incidenten. De beveiligingsmedewerker is ook de contactpersoon voor vragen van betrokkenen.

Domeinverantwoordelijke / proceseigenaar

Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is het betreffende hoofd van de afdeling (vestigingsdirecteur, schoolleider, hoofd stafafdeling) verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze proceseigenaar is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot privacygevoelige persoonsgegevens. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- Samen met het College van Bestuur stellen zij het beleid voor toegang vast.
- Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn
- Samen met functioneel beheer en ICT-beheer beoordelen zij regelmatig de toegangsrechten van gebruikers.

Leidinggevenden hebben een voorbeeldrol ten opzichte van hun medewerkers.

5.1.3. *Uitvoerend*

Security Officer (bij Csg Jan Arentsz belegd bij de systeembeheerder)

De Security Officer vormt een technisch aanspreekpunt inzake informatiebeveiliging voor het management en de medewerkers.
Functioneel beheerder (bij Csg Jan Arentsz belegd bij applicatiebeheerders voor Magister; AFAS financieel; AFAS HRM; Moodle; GoogleforEducation). Zie overzicht gegevensvastleggingen.
De functioneel beheerder wordt vanuit de domeinverantwoordelijke / proceseigenaar voorzien van informatie om zijn taken uit te kunnen voeren.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in de bijlage bij het Veiligheidsbeleidsplan; "Verantwoord omgaan met informatie en sociale media".
Medewerkers wordt gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid.

Leidinggevende
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de manager IBP.

6. **Controle en rapportage**
De functionaris voor gegevensbescherming levert jaarlijks een overzicht van de geregistreerde incidenten aan de directie. Op basis daarvan wordt het informatiebeveiligings- en privacybeleid geëvalueerd en zonodig bijgesteld door de directie/CvB.

Ook n.a.v. actuele gebeurtenissen kan de schoolleiding besluiten om het informatiebeveiligings- en privacybeleid bij te stellen.

6.1. ***Voorlichting en bewustzijn***
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens de belangrijkste speler. Daarom wordt bij Csg Jan Arentsz het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Daartoe worden actuele gebeurtenissen en risico's via weekberichten (of zo nodig per mail) aan de medewerkers kenbaar gemaakt. Indien noodzakelijk worden ook ouders/leerlingen op de hoogte gesteld van IBP-incidenten en de aanpak door de school.

6.2. ***Classificatie en risicoanalyse***
Bij Csg Jan Arentsz heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang zijn voor de informatievoorziening.

6.3. *Incidenten en datalekken*

Alle incidenten t.a.v. IBP dienen te worden gemeld bij Veiligheid@ja.nl (of mondeling bij de functionaris voor gegevensbescherming). De afhandeling van deze incidenten gebeurt onder regie van de functionaris voor gegevensbescherming. Indien nodig zal de FG een melding datalekken doen. (zie procedure melding datalekken).

6.4. *Controle, naleving en sancties*

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van de Informatiebeveiliging en Privacy. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en medewerkers aanspreken in geval van tekortkomingen. Bij tekortkomingen door leerlingen ligt de signalerende en aansprekende rol in eerste instantie bij de betreffende docent in wiens klas de tekortkoming is geconstateerd. Afhankelijk van de situatie kan de docent daar mentor/schoolleider en/of deskundigen bij betrekken. Bij Csg Jan Arentsz wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode (zorgvuldig omgaan met informatie en sociale media), met periodieke bewustwordingscampagnes via de weekberichten, et cetera.
Voor de bevordering van de naleving van de Algemene verordening gegevensbescherming vervult de Functionaris voor Gegevensbescherming (bij Csg Jan Arentsz de Beveiligingsmedewerker) een belangrijke rol. Deze is aangesteld door de College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.
Mocht de naleving ernstig tekort schieten, dan kan Csg Jan Arentsz de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Bij Csg Jan Arentsz is het melden van beveiligingsincidenten vastgelegd in het veiligheidsbeleidsplan, hoofdstuk 10 Procedure data lekken

Tabel IBP rollen en taken

Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
Richtinggevend (strategisch)	CvB Directeur BV	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Privacyreglement vaststellen
Sturend (tactisch)	Manager IBP (bij dir BV)	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen	Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Bewerkersovereenkomsten regelen

		• Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	• Brief toestemming gebruik foto's en video • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Protocol Sociale media • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming (bij Beveiligingsmedewerker)	• Toezicht op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Meldpunt datalekken • Registratie beveiligingsincidenten
	Domeinverantwoordelijke/ Proceseigenaren waaronder: ict, personeel (HRM / P&O), Facilitair, onderwijs, financiën, inkoop en administratie	• **Classificatie / risicoanalyse** *in samenwerking met Manager IBP, ICT-coördinator onderwijs en security officer* • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door *CvB/directie* • *Samen met functioneel beheer en ICT beheer* er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • *Samen met functioneel beheer en ICT* beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) • Classificatie- en risicoanalyse documenten per applicatie/leverancier Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

Uitvoerend (operationeel)	Security officer (Bij hoofd ICT&OW ondersteuning en systeembeheerder) Functioneel beheerders Medewerker Dagelijkse leiding / leidinggevende / directie	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	Communiceren, informeren en toezien op naleving van o.a.: a. IBP in het algemeen b. Regels passend onderwijs c. Hoe omgaan met leerling dossiers d. Wie mogen wat zien e. Gedragscode f. Protocol sociale media g. Mediawijs maken

12. Privacyreglement CSG Jan Arentsz

2. Definities:

Persoonsgegevens	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
Verwerking van persoonsgegevens	Eke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
Bijzonder Persoonsgegeven	Een persoonsgegeven dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid of zijn gezondheid;
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft al dan niet vertegenwoordigd door diens wettelijk vertegenwoordiger. In dit reglement gaat het om de leerlingen en de medewerkers**;**
Wettelijk vertegenwoordiger	Indien de betrokkene de leeftijd van zestien jaren nog niet heeft bereikt, wordt de betrokkene vertegenwoordigd door zijn wettelijk vertegenwoordiger. Meestal zal dit een ouder zijn maar het kan hier ook gaan om een voogd;
Verantwoordelijke	De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Dit is de rechtspersoon waar de Csg Jan Arentsz onder valt, vertegenwoordigd door het bevoegd gezag.
Bewerker	Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
Derde	Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;
School	De verantwoordelijke onderwijsinstelling / bevoegd gezag van Csg Jan Arentsz
3. Reikwijdte en doelstelling	1. Dit reglement stelt regels over de verwerking van persoonsgegevens van leerlingen en medewerkers van Csg Jan Arentsz. 2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door Csg Jan Arentsz worden verwerkt. Dit reglement heeft tot doel: a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens; b. vast te stellen welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt; c. de zorgvuldige verwerking van persoonsgegevens te waarborgen; d. de rechten van betrokkene te waarborgen.

4.Doelen v/d verwerking van de persoonsgegevens	Bij de verwerking van persoonsgegevens houdt Csg Jan Arentsz zich aan de relevante wetgeving waaronder de Algemene verordening gegevensbescherming.
Doelen	De verwerking van persoonsgegevens vindt plaats voor de doelen zoals beschreven in de bijlagen 1, 2 en 3.
5. Doelbinding	Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. Csg Jan Arentsz verwerkt niet meer gegevens dan noodzakelijk is om die vastgestelde doelen te bereiken.
6. Soorten gegevens	De door de Csg Jan Arentsz gebruikte categorieën van persoonsgegevens worden in de bijlagen opgesomd.
7. Grondslag Verwerking	Verwerking van persoonsgegevens gebeurt alleen op grond van: a. Toestemming: in het geval de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend b. Overeenkomst: in het geval de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst c. Wettelijke verplichting: in het geval *de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan Csg Jan Arentsz onderworpen is* d. Vitaal belang: e. Publiekrechtelijke taak: in het geval de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt f. Gerechtvaardigd belang.
8. Bewaartermijnen	Csg Jan Arentsz bewaart de gegevens niet langer dan dat zij noodzakelijk zijn voor het vervullen van het doel waarvoor zij zijn verkregen, tenzij er een andere wettelijke verplichting is die het langer bewaren van de gegevens verplicht stelt.
9. Toegang	Csg Jan Arentsz verleent slechts toegang tot de in de administratie en systemen van Csg Jan Arentsz opgenomen persoonsgegevens aan: a. de bewerker en de derde die onder rechtstreeks gezag van Csg Jan Arentsz staat; b. de bewerker die gemachtigd is om persoonsgegevens te verwerken; c. derden die op grond van de wet toegang moet worden verleend, waarbij alleen toegang wordt verleend aan de gegevens waartoe volgens de wet toegang toe moet worden gegeven.
10. Beveiliging en geheimhouding	a. Csg Jan Arentsz neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. b. Csg Jan Arentsz zorgt dat medewerkers niet meer inzage of toegang hebben tot de persoonsgegevens dan zij strikt noodzakelijk nodig hebben voor de goede uitoefening van hun werk.

	c. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging. Daarbij houdt Csg Jan Arentsz rekening met de concrete risico's die van toepassing kunnen zijn op de verwerkte persoonsgegevens. d. Iedereen die betrokken is bij de uitvoering van dit reglement, en daarbij de beschikking krijgt over persoonsgegevens die vertrouwelijk zijn of geheim moeten worden gehouden (zoals bijvoorbeeld zorggegevens), en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die persoonsgegevens daarvan. e. De verantwoordelijke zal conform de Meldplicht datalekken de Autoriteit Persoonsgegevens onverwijld in kennis stellen van een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. f. De verantwoordelijke zal conform de meldplicht datalekken de betrokkene onverwijld in kennis stellen van de inbreuk bedoeld onder e als de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. g. Een ieder die betrokken is bij de uitvoering van dit reglement en op de hoogte raakt van een (mogelijk) inbreuk op de beveiliging zoals bedoeld onder e is verplicht hiervan onverwijld melding te maken bij de verantwoordelijke. (via de veiligheidscoördinator, per e-mail).
11. Verstrekken gegevens aan derden	Gegevens worden slechts verstrekt aan derden indien de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend, de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is en/of de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene.
12. Sociale media	Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het 'protocol zorgvuldig omgaan met informatie en sociale media' van Csg Jan Arentsz.
13. Rechten betrokkenen	1. De Algemene verordening gegevensbescherming geeft de betrokkene een aantal rechten. Csg Jan Arentsz erkent deze rechten en handelt in overeenstemming met deze rechten.
Inzage	a. Elke betrokkene heeft recht op inzage van de door Csg Jan Arentsz verwerkte persoonsgegevens die op hem/haar betrekking hebben. Csg Jan Arentsz kan vragen om een geldig identiteitsbewijs ter verificatie van de identiteit van de verzoeker
Verbetering, aanvulling, verwijdering en afscherming	a. Betrokkene kan een verzoeken doen tot verbetering, aanvulling, verwijdering of afscherming van zijn persoonsgegevens, tenzij er een wettelijke verplichting tot behoud van de gegevens is, dit onmogelijk blijkt of een onredelijke inspanning zou vergen.
Verzet	b. Voor zover Csg Jan Arentsz persoonsgegevens gebruikt op de grond van artikel 7 onder e en f, dan kan de betrokkene zich verzetten tegen

	verwerking van persoonsgegevens op basis van diens persoonlijke omstandigheden.
Termijn	2. Csg Jan Arentsz dient binnen een termijn van 4 weken na ontvangst van een verzoek daar schriftelijk gehoor aan te geven dan wel deze schriftelijk, gemotiveerd af te wijzen. Csg Jan Arentsz kan de betrokkene laten weten dat er meer tijd nodig is en deze termijn verlengen met maximaal 4 weken.
Uitvoeren verzoek	3. Indien het verzoek van de betrokkene wordt gehonoreerd, draagt Csg Jan Arentsz zorg voor het zo spoedig mogelijk doorvoeren van de verzochte wijzigingen.
Intrekken toestemming	4. Voor zover voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijde door de wettelijk vertegenwoordiger worden ingetrokken.
14. Transparantie	1. Csg Jan Arentsz informeert de betrokkene over de verwerking van zijn persoonsgegevens. Indien het type verwerking dat vraagt, informeert de Csg Jan Arentsz iedere betrokkene apart over de details van die verwerking. 2. Csg Jan Arentsz informeert de betrokkene – op hoofdlijnen – ook over de afspraken die gemaakt zijn met derden en bewerkers die persoonsgegevens van de betrokkene ontvangen.
15. Klachten	1. Wanneer betrokkene van mening is dat het doen of nalaten van Csg Jan Arentsz niet in overeenstemming is met de wetgeving of dit reglement, dan kan betrokkene zich wenden tot het bevoegd gezag van Csg Jan Arentsz. 2. Overeenkomstig de Algemene verordening gegevensbescherming kan de betrokkene zich eveneens wenden tot de rechter of de Autoriteit Persoonsgegevens.
16. Onvoorziene situatie	Indien er zich een situatie voordoet die niet beschreven is in dit reglement dan neemt de verantwoordelijke de benodigde maatregelen rekening houdend met actuele wet- en regelgeving.
17. Wijzigingen reglement	1. Dit reglement wordt na instemming door de MR vastgesteld door de verantwoordelijke. De verantwoordelijke maakt dit reglement openbaar via de website van de school. De verantwoordelijke heeft het recht dit reglement, met instemming van de MR te wijzigingen.
18. Slotbepaling	Dit reglement wordt aangehaald als “het privacyreglement van Csg Jan Arentsz” en treedt in werking in februari 2018**.**

Bijlage 1: Administratie leerlingen

1. De verwerking geschiedt slechts voor de volgende doelen:
   a. De organisatie of het geven van het onderwijs, de begeleiding van leerlingen, dan wel het geven van studieadviezen;
   b. Het verstrekken of ter beschikking stellen van leermiddelen;
   c. Het bekend maken van informatie over de organisatie en leermiddelen, bedoeld onder a en b, alsmede informatie over de leerlingen, bedoeld onder a, op de eigen website;
   d. Het bekendmaken van de activiteiten van de instelling op de eigen website;
   e. Het berekenen, vastleggen en innen van vrijwillige ouderbijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen;
   f. Het behandelen van geschillen en het doen uitoefenen van accountantscontrole;
   g. Het onderhouden van contacten met de oud-leerlingen en oud-medewerkers van de verantwoordelijke;
   h. Andere dan de onder a tot en met g bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van de geldende wet- en regelgeving.

2. Geen andere gegevens worden verwerkt dan:
   a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de betrokkene;
   b. het persoonsgebonden nummer (BSN);
   c. nationaliteit en geboorteplaats;
   d. gegevens als bedoeld onder a, van de wettelijk vertegenwoordiger of verzorger van de leerling;
   e. gegevens betreffende de gezondheid of het welzijn van de leerling voor zover die noodzakelijk zijn voor passende ondersteuning;
   f. gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor de school, het onderwijs of de te geven ondersteuning;
   g. gegevens betreffende de aard en het verloop van het onderwijs en ondersteuning, alsmede de behaalde studieresultaten;
   h. schoolgegevens (waaronder naam school, naam zorgcoördinator/mentor/ intern begeleider, klas/groep waarin de leerling zit, tijdstip van inschrijving bij deze school, naam van de indiener van de aanmelding bij het samenwerkingsverband, schoolloopbaan en rapportage vanuit primair en voortgezet onderwijs);
   i. aanleiding voor de aanmelding bij het samenwerkingsverband, relevante screenings- en onderzoeksgegevens en omschrijving van de problematiek die aan de orde is;
   j. activiteiten die door de school zijn ondernomen rond de betreffende leerling, alsmede de resultaten hiervan;
   k. bestaande of (relevante) afgesloten hulpverleningscontacten en de namen van contactpersonen;
   l. relevante persoonsgegevens die door externe partijen worden verstrekt met betrekking tot de aangemelde problematiek van de betreffende leerling;
   m. relevante financiële gegevens over bijvoorbeeld de vrijwillige ouderbijdrage;

Bijlage 2 Administratie Sollicitanten

1. De verwerking geschiedt slechts voor de volgende doelen:
    a. de beoordeling van de geschiktheid van betrokkene voor een functie die vacant is of kan komen;
    b. de afhandeling van de door de sollicitant gemaakte onkosten;
    c. de interne controle en de bedrijfsbeveiliging;
    d. de uitvoering of toepassing van een andere wet.

2. Geen andere gegevens worden verwerkt dan:
    a. de in bijlage 1 onder a, b en c genoemde gegevens;
    b. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
    c. gegevens als bedoeld onder a, van de ouders, voogden of verzorgers van minderjarige sollicitanten;
    d. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
    e. gegevens betreffende de functie waarnaar gesolliciteerd is;
    f. gegevens betreffende de aard en inhoud van de huidige dienstbetrekking, alsmede betreffende de beëindiging ervan;
    g. gegevens betreffende de aard en inhoud van de vorige dienstbetrekkingen, alsmede betreffende de beëindiging ervan;
    h. andere gegevens met het oog op het vervullen van de functie, die door de betrokkene zijn verstrekt of die hem bekend zijn;
    i. andere dan de onder a tot en met g bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van geldende wet- en regelgeving.

Bijlage 3 Administratie personeel, salaris, uitdiensttreding en pensioen

1. De verwerking geschiedt slechts voor de volgende doelen:
    a. het geven van leiding aan de werkzaamheden van betrokkene;
    b. de behandeling van personeelszaken;
    c. het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura aan of ten behoeve van betrokkene;
    d. het regelen van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband, waaronder de berekening, de vastlegging en de betaling van deze uitkeringen aan of ten behoeve van de betrokkenen;
    e. het berekenen, vastleggen en betalen van belasting en premies ten behoeve van betrokkene;
    f. het vastleggen van een voor de betrokkene geldende arbeidsvoorwaarde;
    g. de opleiding van betrokkene;
    h. de bedrijfsmedische zorg voor betrokkene;
    i. het bedrijfsmaatschappelijk werk;
    j. de verkiezing van de leden van een bij wet geregeld medezeggenschapsorgaan;
    k. de interne controle en de bedrijfsbeveiliging;
    l. de uitvoering van een voor de betrokkene geldende arbeidsvoorwaarde;
    m. het opstellen van een lijst van data van verjaardagen van betrokkenen en andere feestelijkheden en gebeurtenissen;
    n. het verlenen van ontslag;
    o. de administratie van de personeelsvereniging en van de vereniging van oud-personeelsleden;
    p. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen;
    q. het behandelen van geschillen en het doen uitoefenen van accountantscontrole;
    r. andere dan de onder a tot en met q bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van geldende wet- en regelgeving.

2. Geen andere persoonsgegevens worden verwerkt dan:
    a. de in bijlage 1 onder a, b en c genoemde gegevens;
    b. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
    c. gegevens als bedoeld onder a, van de ouders, voogden of verzorgers van minderjarige werknemers;
    d. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
    e. gegevens betreffende de functie of de voormalige functie, alsmede betreffende de aard, de inhoud en de beëindiging van het dienstverband;
    f. gegevens met het oog op de administratie van de aanwezigheid van de betrokkenen op de plaats waar de arbeid wordt verricht en hun afwezigheid in verband met verlof, arbeidsduurverkorting, bevalling of ziekte, met uitzondering van gegevens over de aard van de ziekte;
    g. gegevens met het oog op het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura aan of ten behoeve van de in het eerste lid bedoelde personen;
    h. gegevens met het oog op het berekenen, vastleggen en betalen van belasting en premies ten behoeve van betrokkene;

i. gegevens, waaronder begrepen gegevens betreffende gezinsleden en voormalige gezinsleden van de betrokkenen, die noodzakelijk zijn met het oog op een overeengekomen arbeidsvoorwaarde;
j. gegevens die in het belang van de betrokkenen worden opgenomen met het oog op hun arbeidsomstandigheden;
k. gegevens met oog op het organiseren van de personeelsbeoordeling en de loopbaanbegeleiding, voor zover die gegevens bij de betrokkenen bekend zijn;
l. andere dan de onder a tot en met k bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet.

Bevoegdheden Magister

Een gedetailleerd overzicht van de bevoegdheden op naam functionaris is op verzoek in te zien bij de applicatiebeheerder bij de leerlingadministratie.

	docent	mentor	schoolleider	decaan	zorg coördinator	vestigingsdirecteur	administratie	veiligheidscoördinator
leerlingen vak	x							
leerlingen mentorklas		x						
leerlingen onder team			x					
Leerlingen onder vestiging				x	x	x		
Leerlingen van alle vestigingen							x	x

Bevoegdheden Afas

Een gedetailleerd overzicht van de bevoegdheden op naam functionaris is op verzoek in te zien bij de applicatiebeheerder Afas.

	personeel team / stafafdeling	personeel vestiging	alle personeel	oud-personeel	sollicitanten
schoolleider / hoofd stafafdeling	x				
vestigingsdirecteur	x	x			

voorzitter CvB	x	x	x		
Directeur Oplis	x	x	x		
Coördinator Oplis	x	x	x		
Medewerker P&O	x	x	x	x	x
Medewerker financiële administratie	x	x	x	x	x
Controller	x	x	x	x	x
Medewerker P&V	x	x	x		
Applicatiebeheerder	x	x	x	x	
Leden sollicitatiecommissie					x

13. Wat als je een zwakke plek vindt in een van onze systemen?
Bij Csg Jan Arentsz vinden wij de veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Als jij een zwakke plek in één van onze systemen hebt gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met jou samenwerken om de leerlingen, medewerkers en de informatie in onze systemen beter te kunnen beschermen.

Wij vragen jou:

- Je bevindingen te mailen naar Veiligheid@ja.nl of deze te melden bij de helpdesk bij ICT- en Onderwijsondersteuning;
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer informatie te downloaden dan nodig is om het lek aan te tonen of informatie van leerlingen, docenten of andere medewerkers in te kijken, te delen, te verwijderen of aan te passen;
- De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle informatie die verkregen is via het lek direct na het melden (en indien nodig overdragen van de informatie) van het lek te wissen;
- Geen gebruik te maken van aanvallen op de beveiliging en de internetvoorziening van de school;
- De veiligheidscoördinator/helpdesk van Csg Jan Arentsz voldoende informatie te geven om het probleem te kunnen vinden zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij meer ingewikkelde kwetsbaarheden kan extra informatie nodig zijn.

Wij beloven dat:

- Je binnen 3 werkdagen van ons te horen krijgt dat (en zo mogelijk hoe) we de kwetsbaarheid gaan oppakken;
- Wij je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid;
- Als je de kwetsbaarheid direct na constateren gemeld hebt en via de bovenstaande stappen gehandeld hebt, wij tegen jou geen melding/aangifte zullen doen bij de politie*;
- Jouw melding door ons vertrouwelijk wordt behandeld en dat jouw persoonlijke gegevens niet zonder jouw toestemming met anderen gedeeld worden (tenzij dit wettelijke verplicht is);
- Wij het waarderen wanneer je een kwetsbaarheid meldt en daar een passende beloning tegenover stellen

* Let op: ons beleid voor het melden van zwakke plekken is geen uitnodiging om ons netwerk uitgebreid te scannen om deze te ontdekken.

Constateer je iets waarvan je vermoedt dat het niet klopt meld dat dan direct bij veiligheid@ja.nl **of de helpdesk.** Zo verklein je in ieder geval de kans dat je tijdens jouw 'zoektocht' onbedoeld handelingen uitvoert die mogelijk strafbaar zijn.

Geschreven door Floor Terra (responsibledisclosure.nl), bewerkt door Kennisnet en Csg Jan Arentsz.